MASTER'S THESIS

Het preventief aanpakken van mobile phishing naar beveiligingscodes in Nederland

Het elimineren van mobile phishing aanvallen door de grondoorzaken van dit probleem te achterhalen

Bujitu, L.

Award date:
2021

Het preventief aanpakken van mobile phishing naar beveiligingscodes in Nederland

Het elimineren van mobile phishing aanvallen door de grondoorzaken van dit probleem te achterhalen.

Student:	Linda Bujitu
Studentnummer:	
Datum:	15-04-2021
Afstudeerbegeleider:	Lex Bijlsma
Meelezer:	LIoyd Rudledge
Versie :	7.0
Status:	compleet

Het preventief aanpakken van mobile phishing naar beveiligingscodes in Nederland

Het elimineren van mobile phishing aanvallen door de grondoorzaken van dit probleem te achterhalen.

Preventive tackling mobile phishing for security codes for internet banking in the Netherlands

Eliminating mobile phishing attacks by finding the root causes of this problem.

Opleiding:	Open Universiteit, faculteit Betawetenschappen Masteropleiding Business Process Management & IT
Degree programme:	Open University of the Netherlands, Faculty Science Master of Science Business Process Management & IT
Course:	IM0602 BPMIT Graduation Assignment Preparation IM9806 Business Process Management and IT Graduation Assignment
Student:	Linda Bujitu
Identificatie number:	
Date:	06-04-2021
Thesis supervisor	Lex Bijlsma
Second reader	LIoyd Rudledge
Version number:	7.0
Status:	complete

Abstract

Mobile phishing is a form of cyber attacks that criminals use to tempt smartphone users to click on a link via WhatsApp, SMS or Messenger, for example, and to log in to a false (bank) website with personal details such as username and password for further exploitation. In recent years, the problem of mobile phishing for internet banking security codes has increased. Especially in times of Corona (2020-2021) this problem has increased significantly. This research is aimed at investigating how mobile phishing for internet banking security codes can be prevented. Data was collected by conducting a literature search, sending out a survey and mailing a questionnaire to a Dutch bank. The findings of this research are that little literature can be found about mobile phishing in the Netherlands, while this problem is increasing in times of Corona. For example, it appears that the process of mobile phishing has not been fully mapped out in previous studies and it is not clear exactly what measures banks and potential victims are taking to combat this problem. The results of the empirical research largely confirm the results of existing literature. Further research into causes and prevention measures for this problem is required to combat this problem.

Sleutelbegrippen

Mobile phishing, smishing, phishing, beveiligingscodes internetbankieren, betaalverzoekfraude

Samenvatting

De afgelopen jaren is het probleem mobile phishing naar beveiligingscodes voor internetbankieren toegenomen. Vooral in tijden van Corona (2020-2021) is dit probleem aanzienlijk toegenomen. Smartphones zijn namelijk aantrekkelijke middelen voor cybercriminelen voor het plegen van mobile phishing. Daarnaast is het tegenwoordig eenvoudig om als Nederlandse burger zelf een mobile phishing aanval te plegen en hier dus geld mee te verdienen.

Mobile phishing is een vorm van cyberaanvallen waarmee criminelen smartphone users verleiden om via whatsapp, sms of bijvoorbeeld Messenger op een link te klikken en op een valse (bank) website in te loggen met persoonlijke gegevens zoals gebruikersnaam, wachtwoord voor verdere exploitatie.

Dit onderzoek is gericht op het onderzoeken van hoe mobiele phishing naar beveiligingscodes voor internetbankieren tegengegaan kan worden. Om die reden staat de volgende onderzoeksvraag centraal in dit onderzoek:

Wat moet er in Nederland gebeuren om mobile phishing naar beveiligingscodes voor internetbankieren tegen te gaan?

Voor het beantwoorden van de onderzoeksvraag, is als eerst literatuuronderzoek verricht. Aan de hand van literatuuronderzoek is het proces van mobile phishing in kaart gebracht en zijn mogelijke oorzaken dat slachtoffers op een phishing link klikken onderzocht. Na het uitvoeren van literatuuronderzoek is een empirisch onderzoek verricht. Een vragenlijst is gemaild naar een Adviseur Fraud & Corporate Security van een Nederlandse bank en een enquête is uitgestuurd naar potentiële slachtoffers die in Nederland wonen. Aan de hand van dataverzameling in het empirisch onderzoek is in kaart gebracht hoe slachtoffers tegen het probleem aankijken en welke maatregelen banken precies treffen om het probleem mobile phishing naar beveiligingscodes voor internetbankieren tegen te gaan. Tenslotte is gekeken in hoeverre de resultaten van het empirisch onderzoek de resultaten van het literatuuronderzoek bevestigen en / of aanvullen.

Het antwoord op de onderzoeksvraag is dat dit probleem aangepakt kan worden door als eerst meer onderzoek te verrichten naar het proces van mobile phishing en naar hoe de verspreiding van mobile phishing pakketten tegengegaan kan worden. Daarnaast dienen Nederlandse banken verder te onderzoeken hoe de online betaalomgeving via de webbrowser beter beveiligd kunnen door bijvoorbeeld extra verificatievragen toe te passen bij het inloggen of 2 factorauthenticatie toe te passen. Ook dient er een beveiligingsmethode ontwikkeld te worden waardoor potentiële slachtoffers direct gewaarschuwd worden dat het om een phishing website gaat en ze niet moeten inloggen met hun bankgegevens.

Aanbevolen wordt dat de politie dit probleem meer prioriteit geeft door bijvoorbeeld in kaart te brengen op welke online platformen mobile phishing pakketten worden aangeboden. Uit zowel literatuur-als empirisch onderzoek kwam namelijk naar voren dat dit probleem steeds meer aan het groeien is in Nederland. Dit komt mede omdat het zo eenvoudig is om aan een mobile phishing pakket te komen en dus een mobile phishing aanval te plegen. Het opsporen van fraudeurs is die de phishing websites bouwen is een manier om de kern van dit probleem aan te pakken. Bovendien wordt aanbevolen om een soortgelijk onderzoek te herhalen en daarbij slachtoffers van mobile phishing te enquêteren. Dan kan bijvoorbeeld onderzocht worden of er een verband is tussen demografische factoren en het slachtofferschap van mobile phishing. Ook dient onderzoek gedaan te worden naar een technologie om phishing websites meteen te detecteren en potentiële slachtoffers een melding geven dat het om een phishing website gaat.

Summary

In recent years, the problem of mobile phishing for internet banking security codes has increased. Especially in times of Corona (2020-2021) this problem has increased significantly. Smartphones are attractive means for cyber criminals to commit mobile phishing. In addition, it is very easy as a Dutch citizen to commit a mobile phishing attack yourself and thus earn money with it.

Mobile phishing is a form of cyber attacks that criminals use to tempt smartphone users to click on a link via WhatsApp, SMS or Messenger, for example, and to log in to a false (bank) website with personal details such as username and password for further exploitation.

This research is aimed at investigating how mobile phishing for internet banking security codes can be prevented. For that reason, the following research question is central to this research:

What should be done in the Netherlands to combat mobile phishing for internet banking security codes?

Literature research was carried out first to answer the research question. Based on literature research, the process of mobile phishing has been mapped out and possible causes that victims click on a phishing link have been investigated. After carrying out a literature search, an empirical study was performed. A questionnaire was emailed to a Fraud & Corporate Security Advisor of a Dutch bank and a survey was sent to potential victims who live in the Netherlands. Based on data collection in the empirical research, it has been mapped out how victims view the problem and what measures banks are taking to combat the problem of mobile phishing for security codes for internet banking. Finally, it was examined to what extent the results of the empirical study confirm and / or supplement the results of the literature study.

The answer to the research question is that this problem can be tackled by first conducting more research into the process of mobile phishing and how the spread of mobile phishing packages can be prevented. In addition, Dutch banks should further investigate how the online payment environment can be better secured via the web browser, for example by applying extra verification questions when logging in or applying 2-factor authentication. A security method should also be developed that immediately warns potential victims that it is a phishing website and that they should not log in with their bank details.

It is recommended that the police give this problem more priority by, for example, identifying the online platforms on which mobile phishing packages are offered. Both literature and empirical research have shown that this problem is growing in the Netherlands. This is partly because it is very easy to get a mobile phishing package and therefore to commit a mobile phishing attack. Detecting the fraudsters who build the phishing websites is one way to tackle the core of this problem. In addition, it is recommended to repeat a similar survey, surveying victims of mobile phishing. Then, for example, it can be investigated whether there is a link between demographic factors and victimization of mobile phishing. Research should also be conducted into a technology to immediately detect phishing websites and notify potential victims that it is a phishing website.

Inhoud

1. Introductie

In dit hoofdstuk wordt onder andere het onderwerp van dit onderzoek geïntroduceerd, achtergrondinformatie gegeven, de relevantie van dit onderzoek onderbouwt en de aanpak in hoofdlijnen toegelicht.

1.1 Achtergrond

RTL-nieuws gaf in 2019 aan dat er in Nederland een grote toename is in mobile phishing via whatsapp, sms of Messenger (van Dijke, 2019) (van Dijke, 2020). De Betaalvereniging Nederland en de Nederlandse Vereniging van Banken (NVB) geven aan dat in de eerste helft van 2019 bankklanten door mobile phishing naar beveiligingscodes ruim 3,1 miljoen euro hebben verloren (van Dijke, 2019). In de zes maanden daarvoor bedroeg dit 2,4 miljoen euro (van Dijke, 2019). Sterker nog in mei 2020 zijn er bij de politie 1.869 meldingen van cybercrime gedaan (van Dijke, 2020). Dit aantal is 6,8 keer meer ten opzichte van dezelfde maand in de afgelopen drie jaar. Het ging dan om oplichting via Marktplaats, whatsapp of om het stelen van inlog- en betaalgegevens (ook wel mobile phishing genoemd) (van Dijke, 2020). Mobile phishing is net zoals bijvoorbeeld ransomware, botnet en cryptojacking een vorm van cybercrime. Cybercrime is een misdaad die gericht is op ICT en wordt gepleegd op een computer, smartphone, tablet, smartwatch of andere digitale middelen. De reden waarom mobile phishing in dit onderzoek de aandacht verdiend is omdat zoals hierboven beschreven mobile phishing in Nederland steeds vaker voorkomt en dit stoppen.

1.2 Gebiedsverkenning

Voorgaande studies tonen aan dat smartphones aantrekkelijke middelen zijn voor cybercriminelen (Verkijika,2019, blz. 28) (Aleroud& Zhou, 2017, blz. 160-198) (Chiew, Yong & Tan, 2018, blz.1-2) (Goel & Jain, 2018, blz. 519-520) (Kadhim & Al-saed, 2017, blz. 349). Hiermee kunnen cybercriminelen immers mobile phishing aanvallen plegen. Tegenwoordig gebruiken mensen namelijk smartphones om activiteiten uit te voeren die voorheen op de desktop werden uitgevoerd. Hierbij kan bijvoorbeeld gedacht worden aan activiteiten zoals internetbankieren of googlen. Google gaf in 2015 aan dat wereldwijd meer zoekopdrachten worden uitgevoerd vanuit smartphones dan via de desktop (Blauwe Monsters, 2015). Verwacht wordt dat deze trend zich zal voorzetten en ook bij bijvoorbeeld internetbankieren. Uit onderzoek van Peachey (2019) is gebleken dat er meer gebruik wordt gemaakt van mobiele bankieren dan internetbankieren via de desktop.

Mobile phishing is als volgt gedefinieerd: *Mobile phishing is een vorm van cyberaanvallen waarmee criminelen smartphone users verleiden om via whatsapp, sms of bijvoorbeeld Messenger op een link te klikken en op een valse (bank) website in te loggen met persoonlijke gegevens zoals gebruikersnaam, wachtwoord voor verdere exploitatie (Aleroud & Zhou, 2017, blz. 160) (Chiew, Yong & Tan, 2018, blz.1) (Goel & Jain, 2018, blz. 519) (Kadhim & Al-saed, 2017, blz. 349) (Choudhary, Jain, 2017, blz. 349) (Khonji, Iraqi & Jones, 2013, blz. 2091).* Hieraan kan toegevoegd worden dat bijvoorbeeld financieel gewin, het stelen van intellectueel eigendom en stelen van gevoelige informatie redenen voor cybercriminelen zijn voor het plegen van mobile phishing (Choudhary, Jain, 2017, blz. 349-356) (Khonji, Iraqi & Jones, 2013, blz. 2091-2121). Aan een link kan men denken aan een link naar een valse website die identiek is aan de website van een bank waardoor potentiële slachtoffers eerder geneigd zijn om in te loggen met bankgegevens.

1.3 Probleemstelling

Mobile phishing is zoals eerder genoemd een probleem in Nederland wat nu in tijden van Corona steeds vaker voorkomt (van Dijke, 2019) (van Dijke, 2020). Hierdoor worden slachtoffers, in dit geval gebruikers van smartphones die zijn getroffen door mobile phishing financieel zwaar getroffen. In

tijden van Corona is de Nederlandse economie achteruitgegaan en zijn veel mensen werkloos geworden. Uit de statistieken van het CBS blijkt namelijk dat gedurende het Corona crisis het werkloosheidspercentage is toegenomen van 3,0 naar 3,8 procent en het aantal openstaande vacatures met maar liefst 30 procent is afgenomen (CBS, 2020). Om als werkloze ook nog eens slachtoffer te worden van mobile phishing is een misère. Mobile phishing in Nederland verdient daarom de aandacht om nader onderzocht te worden. Er zijn talloze voorbeelden van mobiele phishing te noemen zoals; mobile phishing naar beveiligingscodes voor internetbankieren via whatsapp, Marktplaats of Messenger en mobile phishing naar digid gegevens. Dit onderzoek is echter afgebakend tot mobile phishing naar beveiligingscodes voor internetbankieren in Nederland.

1.4 Opdrachtformulering

De opdracht is gericht op het onderzoeken van hoe mobiele phishing naar beveiligingscodes voor internetbankieren tegengegaan kan worden. Om die reden dient de volgende onderzoeksvraag beantwoord te worden:

Wat moet er in Nederland gebeuren om mobile phishing naar beveiligingscodes voor internetbankieren tegen te gaan?

In dit onderzoek zal onderzocht worden hoe het probleem (mobile phishing naar beveiligingscodes voor internetbankieren in Nederland*)* tot de kern aangepakt kan worden. Zo wordt kennis gegenereerd over hoe mobile phishing criminelen precies te werk gaan, teneinde kennis te genereren om deze vorm van mobile phishing te bestrijden. Voor het beantwoorden van de onderzoeksvraag zijn een achttal deelvragen opgesteld:

Theoretische deelvragen
1. Wat is de motivatie van hackers voor het uitvoeren van mobile phishing aanvallen?
2. Hoe komt een mobile phishing aanval naar beveiligingscodes voor internetbankieren tot stand?
3. Wat is de ontwikkeling van mobile phishing naar beveiligingscodes voor internetbankieren van de afgelopen drie jaar in Nederland?
4. Wat zijn de gevolgen van mobile phishing naar beveiligingscodes voor internetbankieren in Nederland?
5. Welke maatregelen hebben Nederlandse banken tot nu toe getroffen om bankklanten te beschermen tegen mobile phishing naar beveiligingscodes voor internetbankieren?
Empirische deelvragen
6. Wat doen de eindgebruikers van smartphones zelf ter beveiliging van hun beveiligingscodes voor internetbankieren?
7. Welke oorzaken beïnvloeden slachtoffers om tijdens het gebruik van hun smartphone op een valse link te klikken en in te loggen met hun bankgegevens?
8. In hoeverre zijn de maatregelen van banken om bankklanten te beschermen tegen mobile phishing naar beveiligingscodes voor internetbankieren bestand genoeg tegen mobile phishing naar beveiligingscodes voor internetbankieren?

1.5 Motivatie/ relevantie

In de bestaande vakliteratuur is informatie terug te vinden over mobile phishing. Toch geven voorgaande studies aan dat er weinig onderzoek is gedaan in dit onderzoeksgebied (Aleroud& Zhou, 2017, blz. 161) (Goel & Jain, 2018, blz. 520). Zo blijkt dat er in Nederland een schaarste is aan wetenschappelijk onderzoek naar mobile phishing in Nederland. Op het internet (Google, Google Scholar, Centraal bureau statistiek (CBS), Fraudehelpdesk) en in krantenartikelen is bijvoorbeeld nergens terug te vinden wat de verhouding is van meldingen van mobile phishing in Nederland tot alle

meldingen van cybercrime in Nederland. Aanvullend op bovengenoemde geeft Henk Hendriks, de directeur van Datacenter services van de Belastingdienst (2020) aan dat het niet bekend is hoeveel slachtoffers zijn getroffen door mobile phishing waarin criminelen zich voordoen als de belastingdienst en hier een sms van versturen. Het onderzoeken van deze vorm van mobile phishing in Nederland is relevant omdat hiermee potentiële slachtoffers meer inzicht krijgen in het herkennen van mobile phishing en banken meer inzicht krijgen in het vinden van passende maatregelen, teneinde empirisch vast te stellen hoe deze vorm van mobile phishing tegengegaan kan worden. Bovendien kunnen de resultaten uit dit onderzoek wereldwijd bruikbaar zijn omdat er wereldwijd smartphone gebruikers zijn die internet bankieren gebruiken (CBS, 2020).

1.6 Aanpak in hoofdlijnen

Eerst is literatuuronderzoek verricht. Het literatuuronderzoek is beschreven in hoofdstuk 2- Theoretisch kader. Vervolgens is de methode van aanpak van dit onderzoek beschreven. De methode en aanpak van dit onderzoek zijn beschreven in hoofdstuk 3- Methodologie. Na het uitvoeren van literatuuronderzoek is een empirisch onderzoek uitgevoerd waarin de bevindingen uit het literatuuronderzoek verder zijn onderzocht. Dit onderzoek is uitgevoerd door het uitsturen van een online enquête en het mailen van een vragenlijst nar een medewerker van een Nederlandse bank die zich dagelijks bezig houdt met beveiligingsvraagstukken van de Nederlandse bank.

Vervolgens zijn de resultaten verwerkt in hoofdstuk 4- Resultaten. Tenslotte eindigt dit rapport in hoofdstuk 5 met conclusies, discussie en aanbevelingen voortvloeiend uit dit onderzoek. Hierin wordt antwoord gegeven op de deelvragen en hoofdvraag. Daarnaast wordt gereflecteerd op de uitvoering van de literatuur- en empirisch onderzoek en worden aanbevelingen gedaan voor de praktijk en vervolgonderzoek.

2. Theoretisch kader

Dit hoofdstuk betreft een beschrijving van het literatuuronderzoek naar mobile phishing naar beveiligingscodes voor internetbankieren in Nederland. Om het literatuuronderzoek vorm te geven zijn in paragraaf 1.4 vijf theoretische deelvragen opgesteld.

2.1 Onderzoeksaanpak

Het doel van de ontwikkeling van het theoretisch kader is om erachter te komen wat er in de bestaande literatuur wel of niet bekend is over mobile phishing naar beveiligingscodes voor internetbankieren.. Er is onderzocht in hoeverre bruikbare informatie van bestaande studies valide en generaliseerbaar is.

Voor het uitvoeren van het literatuuronderzoek is het proces van literatuuronderzoek volgens Saunders, Lewis en Thornhill (2019) toegepast. De eerste stap van het proces betreft het opstellen van onderzoeksvragen en -doelstellingen. Vervolgens zijn onderstaande stappen regelmatig uitgevoerd totdat een kritisch overzicht van de literatuur is verkregen.

1. Definieer de zoekparameters
2. Genereer trefwoorden
3. Voer de zoekopdracht(en) uit
4. Verkrijg literatuur
5. Evalueer de literatuur
6. Maak notities van relevante informatie uit de literatuur

De gedefinieerde parameters zijn terug te vinden in Bijlage 1. Door het uitvoeren van bovengenoemde stappen zijn 20 zoektermen gegenereerd. Zie *Tabel 1*.

2.2 Uitvoering

Met behulp van de zoekmachine Summon is de volgende meest recente en meest geciteerde publicatie opgezocht over mobile phishing: Verkijika, S.F. (2019). “If you know what to do, will you take action to avoid mobile phishing attacks”: Self-efficacy, anticipated regret, and gender’’. Computers in Human Behavior. 101. blz. 28-296. Uit dit artikel zijn de volgende relevante zoektermen geselecteerd. Ook is gezocht naar nieuwsberichten omtrent mobile phishing in Nederland. De gevonden RTL-nieuwsberichten hebben bijgedragen aan het opstellen van de probleemstelling en onderzoeksvraag. Vervolgens zijn tevens zoektermen geselecteerd uit de probleemstelling en onderzoeksvraag van dit onderzoek. Tenslotte is een lijst opgesteld bestaande uit 20 zoektermen (zie *Tabel 1*).. Met behulp van de lijst is doelgericht gezocht naar relevante literatuur.

Tabel 1: zoekresultaten literatuuronderzoek Zoekmachine Summon

Zoekterm	**Zoekresultaten literatuurtekst**	**Zoekresultaten op titel**	**Aantal relevante resultaten**
Mobile phishing attack	5.124	16	2
Mobile phishing	7.327	47	3
Phishing smartphones	1.316	5	4
Benefits mobile phishing	272	1	2
Phishing detection	7.522	218	1
Anti-phishing	2.995	257	0
Social engineering + mobile phishing	1.953	0	1 zoekresultaat literatuurtekst
Mobile phishing + Nederland	15	0	3 zoekresultaten literatuurtekst

Internetbankieren +criminelen	7	0	2
Beveiligingscodes + internetbankieren	0	0	0
Phished people	388	3	1
Smishing	300	24	1
Totaal	26.947	571	19

Zoals in *Tabel 1* weergegeven zijn er in totaal 26.947 resultaten gegenereerd door het zoeken van literatuur tekst met behulp van de opgestelde zoektermen. Echter, om de zoekresultaten verder te verfijnen is literatuur opgezocht door in de zoekmachine Summon te zoeken op titel, wat de zoekresultaten heeft teruggedrongen naar 571. Daaraan kan worden toegevoegd dat er met behulp van de opgestelde zoektermen zowel in het Engels als Nederlands is gezocht naar literatuur. Zoals in *Tabel 1* te zien zijn zoektermen in sommige gevallen gecombineerd om wetenschappelijke artikelen terug te vinden waar alle genoemde termen in de tekst of titel voorkomen.

De sneeuwbal- en citatiemethode is toegepast om relevante literatuur te vinden. Bij het toepassen van de sneeuwbalmethode is een literatuurlijst van een relevant artikel bekeken om nieuwe relevante artikelen te vinden. De citaatmethode is het tegenovergestelde van de sneeuwbalmethode en hierbij is gezocht naar bronnen waarin naar een goed wetenschappelijk artikel is verwezen. Google Scholar geeft bij de zoekresultaten namelijk aan door welke andere artikelen de bron is geciteerd. Naast het raadplegen van Google Scholar en de zoekmachine Summon is via Google recente informatie opgezocht van RTL-nieuwberichten, Nederlandse betaalvereniging en de fraudehelpdesk. De reden hiervan is dat in de bestaande literatuur informatie ontbrak over hoe mobile phishing in Nederland in elkaar zit (feiten en cijfers) en wat Nederlandse banken hiertegen doen (in paragraaf 2.3 wordt hier verder op ingegaan).

Uit de 571 gevonden artikelen zijn uiteindelijk 19 relevante artikelen geselecteerd. De selectie van deze relevante artikelen is gebeurd door te filteren op het aantal citaties, het bestuderen van de inleiding, samenvatting en de conclusies en te kijken naar de publicatiedatum. De bruikbaarheid is bepaald door te kijken of de artikelen in andere artikelen geciteerd zijn, te beoordelen of de artikelen al peer-reviewed zijn en te kijken of het artikel gepubliceerd is in een journal of afkomstig is van een wetenschappelijk instituut. Bij het bestuderen van de inleidingen, samenvattingen en conclusies van de artikelen is gekeken of de informatie goed past bij het onderwerp van dit onderzoek. Tezamen resulteerde dit tot 19 relevante artikelen (exclusief relevante informatie van websites) die verwerkt zijn in het literatuuronderzoek. De publicatiedatum van de artikelen is bekeken om te voorkomen dat achterhaalde informatie in het literatuuronderzoek wordt verwerkt.

2.3 Resultaten en conclusies

In deze paragraaf wordt middels de informatie wat voortvloeit uit het literatuuronderzoek, antwoordt gegeven op de eerste vijf deelvragen van dit onderzoek. Hierna zal een conclusie getrokken worden en wordt vastgesteld wat de bijdrage zal zijn van het vervolgonderzoek.

Vanuit literatuuronderzoek is naar voren gekomen dat cyber criminelen diverse beweegredenen hebben voor het plegen van een mobile phishing. Gebrek aan bewustzijn over de mobile phishing-aanvallen in de samenleving is een van de belangrijkste reden waarom phishing-aanvallen afgelopen jaren zo succesvol zijn geweest (Gupta et al, 2017). De meest voor de hand liggende beweegreden voor het plegen van mobile phishing is financieel gewin (Gupta et al, 2016, blz. 3629) (Verkijika,2019, blz. 28-296). Maar er zijn meerdere beweegreden voor het plegen van mobile phishing zoals;

identiteitsdiefstal, verkopen van adres en contactgegevens, diefstal van bankgegevens, et cetera (Kumar et al, 2018, blz. 510-522). Echter, het uiteindelijke doel is om slachtoffers geld afhandig te maken (Bullée & Junger, 2020). In het onderzoek van Gupta et al (2017) wordt beweerd dat er naast financieel gewin nog een reden is voor het uitvoeren van mobile phishing aanvallen, namelijk beroemdheid en erkenning. Een interessant psychologisch aspect voor het plegen van mobile phishing is om erkenning te krijgen onder leeftijdsgenoten. Het gehele proces van mobile phishing naar beveiligingscodes van beveiligingscodes is beschreven in Bijlage 2. Hierin is te zien dat zelfs mensen met weinig technische kennis, mobile phishing aanvallen kunnen plegen.

Onderzoekers hebben zich beperkt tot een aantal redenen waarom smartphone gebruikers het belangrijkste doelwit zijn van phishing aanvallen. Ten eerste is het op smartphones lastiger om de URL van een website te controleren omdat het scherm van een smartphone vele maal kleiner is dan een scherm van een desktop (Kumar et al, 2018, blz. 510-522) (Verkijika,2019, blz. 28-296). Daarnaast zijn vele smartphone gebruikers niet of onvoldoende op de hoogte van de opties om mobile phishing te voorkomen (Shahriar, Klintic, & Clincy, 2015, blz. 206-212). Bovendien vereisen meer dan 40% van de mobiele applicaties dat gebruikers inloggegevens invoeren met eenvoudige gebruikersinterfaces die gemakkelijk kunnen worden gevolgd door cyber criminelen. Er zijn immers geen veiligheidstoepassing identiteits indicatoren beschikbaar in besturingssystemen en webbrowsers van smartphones (Verkijika,2019, blz. 28-296) (Shahriar, Klintic, & Clincy, 2015, blz. 206-212) (Shahriar et al ,2019, blz. 178-193). Hierdoor kunnen cyber criminelen vrij eenvoudig een valse website bouwen die legitieme gebruikersinterfaces nabootsen, dit zijn zogenoemde phishing panels (Shahriar et al ,2019, blz. 178-193) (Shahriar, Klintic, & Clincy, 2015). Daarnaast geven onderzoekers aan dat de reeds bestaande technische preventiemaatregelen voor mobile phishing niet gericht zijn op de steeds wijzigende manier waarop cyber criminelen hun slachtoffers benaderen (Vijayalakshmi et al, 2020, blz. 235-246) (Shahriar et al ,2019, blz. 178-193)) (Aleroud& Zhou, 2017, blz. 160-198) (Kadhim & Al-saed, 2017, blz. 349) (Goel & Jain, 2018, blz. 519-520) (Bojjagani et al,2020, blz. 1110–1119) (E.M. & A.K., 2019, blz.1-11). Sterker nog Canfield (2016) geeft in zijn onderzoek aan dat ondanks de ontwikkeling van de steeds nieuwe technologische oplossingen, de mens de zwakste schakel blijft.

Afgelopen jaren zijn mobile phishing aanvallen wereldwijd significant toegenomen omdat smartphones door cyber criminelen beschouwd wordt als een aantrekkelijk middel voor het plegen van phishing aanvallen (Verkijika,2019, blz. 28) (Aleroud& Zhou, 2017, blz. 160-198) (Chiew, Yong & Tan, 2018, blz.1-2) (Goel & Jain, 2018, blz. 519-520) (Kadhim & Al-saed, 2017, blz. 349). Gebrek aan bewustzijn over mobile phishing in de samenleving is ook de belangrijkste reden waarom mobile phishing-aanvallen zo succesvol zijn geweest (Verkijika,2019, blz. 28) (Vishwanatha et al, 2011, blz. 576-586). In Nederland is het aantal mobile phishing aanvallen naar beveiligingscodes voor internetbankieren vooral tijdens de coronacrisis enorm toegenomen. Echter, het precieze aantal en toename in mobile phishing naar beveiligingscodes voor internetbankieren in Nederland is niet bekend. Volgens de fraudehelpdesk en politie komt dit omdat niet alle (potentiële) slachtoffers dit melden. Maar RTL-nieuws gaf in 2020 het volgende aan: ‘De afgelopen jaren neemt het aantal cybercrime-meldingen al gestaag toe, maar sinds de coronacrisis is uitgebroken, gaat het pas echt door het dak. Het gaat dan bijvoorbeeld om oplichting via Marktplaats of WhatsApp, of om het stelen van inlog- en betaalgegevens (phishing)’. Daarnaast gaf van Dijke (2020) aan dat Nederlandse banken de laatste tijd opvallend veel meldingen ontvangen van klanten over phishing via mobiele berichtendiensten zoals sms, WhatsApp en Messenger.

Mobile phishing naar beveiligingscodes voor internetbankieren heeft gevolgen voor slachtoffers. Aleroud & Zhou (2017) geven in hun onderzoek aan dat bovengenoemde vorm van mobile phishing de volgende ernstige gevolgen kan hebben voor de slachtoffers: het verlies van gevoelige informatie en

financieel verlies. Vooral het financieel verlies weegt zwaar voor de slachtoffers (Vishwanatha et al, 2011, blz. 576-586). Echter is in de literatuur niet helemaal bekend hoeveel financiële schade slachtoffers in Nederland in totaal hebben geleden aan mobile phishing naar beveiligingscodes van internetbankieren. In de jaarrekening van Stichting aanpak financieel-economische criminaliteit in Nederland (2019) is vermeld dat slachtoffers van alle fraudemeldingen in totaal 26.177.622 euro aan financiële schade hebben geleden. Aangezien 34,87 procent van alle meldingen omtrent mobile phishing naar beveiligingscodes voor internetbankieren bedroeg, wordt geschat dat slachtoffers in 2019 9.128.136,79 euro aan financiële schade hebben geleden (Fraudehelpdesk, 2019). Op de website van de betaalvereniging van Nederland (2020) staat tevens dat door phishing naar beveiligingscodes voor internetbankieren bij bankklanten vorig jaar meer dan verdubbeld is, van 3,81 miljoen euro in 2018 tot 7,94 miljoen euro in 2019. Dit is slechts een ruwe schatting waar een afwijking in kan zijn omdat niet alle slachtoffers van mobile phishing dit melden bij de Fraudehelpdesk of politie. Aangenomen wordt dat naast financiële gevolgen er meer gevolgen zijn zoals gevolgen op psychisch vlak. Het kan namelijk voorkomen dat slachtoffers er heel lang mee zullen worstelen.

Banken zijn voortdurend aan het investeren in strengere bewaking van alle online transacties. Zo blijkt dat banken proberen verdachte ongebruikelijke transacties bij klanten tijdig te herkennen. Als de bank een verdachte transactie heeft vastgesteld, neemt de bank contact op met de klant (veilig bankieren, 2020). Daarnaast zijn de apps van banken veiliger geworden omdat er een mogelijkheid is om met vingerafdruk of gezichtsherkenning in te loggen in de app van de bank. Voor de valse websites (phishing panels) is geen maatregel van banken teruggevonden. Deze phishing panels gaan binnen 24 uur al uit de lucht omdat criminelen deze snel verwijderen. Nederlandse banken geven aan dat de eigen inzet en waakzaamheid van bankklanten ook van belang blijft om mobile phishing aanvallen naar beveiligingscodes voor internetbankieren terug te dringen (Betaalvereniging Nederland, 2020). Hiervoor geven banken doorlopende voorlichtingscampagnes over veel voorkomende phishing aanvallen om zo bankklanten te waarschuwen voor allerlei vormen van phishing. Echter is het niet inzichtelijk hoe effectief de huidige maatregelen van banken zijn en in hoeverre deze kenbaar zijn onder de Nederlandse bevolking.

De conclusie die uit het literatuuronderzoek gesteld kan worden is dat op wetenschappelijk vlak nauwelijks is aangetoond hoe het proces van mobile phishing naar beveiligingscodes voor internetbankieren (in Nederland) er precies uitziet. In het artikel van Rooyakkers en Kranenborg (2020) is het proces van ‘betaalverzoekfraude via marktplaats’ in hoofdlijnen weergegeven in een afbeelding. Betaalverzoekfraude is een strafbaar feit wat gepleegd wordt door het plegen van (mobile) phishing naar beveiligingscodes voor internetbankieren. Echter, met behulp van informatie uit diverse artikelen is het wel gelukt om het proces hiervan inzichtelijk te maken (zie *Bijlage 1*). Daarnaast ligt de focus van voorgaande onderzoeken veelal op technieken om phishing websites te detecteren en mogelijk te elimineren en op de factoren die van invloed zijn op het slachtofferschap van mobile phishing. Er is ook geen survey- of fieldonderzoek in Nederland uitgevoerd (althans niet teruggevonden) waarin bijvoorbeeld onderzocht is hoe de Nederlandse bevolking deze vorm van mobile phishing ervaart en of er hiervan voldoende bewustwording en kennis is onder de Nederlandse bevolking. Ook is geen inhoudelijke informatie teruggevonden over wat Nederlandse banken tot nu toe precies hebben uitgevoerd om bankklanten te beschermen tegen deze vorm mobile phishing.

2.4 Doel van het vervolgonderzoek

Het doel van het vervolgonderzoek is om de volgend zaken omtrent mobile phishing naar beveiligingscodes voor internetbankieren middels empirisch onderzoek in kaart te brengen:

- In welke mate potentiële slachtoffers de inloggegevens van hun smartphone beveiligen.

- Welke gevolgen voor banken en slachtoffers allemaal gepaard gaan met dit probleem.
- Wat Nederlandse banken precies in de huidige situatie doen om bankklanten te beschermen tegen dit probleem.
- Hoe effectief deze huidige maatregelen van banken zijn.

Dit onderzoek is dus exploratief van aard. Mogelijk zullen hypothesen uit dit vervolgonderzoek voortvloeien die later met behulp van ander onderzoek getest kunnen worden.

3. Methodologie

In dit hoofdstuk wordt uitgelegd hoe het empirisch onderzoek wordt uitgevoerd. Eerst worden de onderzoeksstrategie en onderzoeksmethoden toegelicht. Vervolgens wordt toegelicht hoe de betrouwbaarheid en validiteit van dit onderzoek wordt gewaarborgd en hoe binnen dit onderzoek rekening wordt gehouden met ethische aspecten.

3.1 Conceptueel ontwerp: keuze van onderzoeksmethode(n)

De onderzoeksstrategie is inductief omdat er weinig in de literatuur terug te vinden is om deelvraag 6 tot en met 8 te beantwoorden. Er wordt vanuit een specifieke observatie gekeken of generalisatie vastgesteld kan worden. Hiervoor worden de onderzoeksmethoden survey- en veldonderzoek toegepast. Enquêtes worden afgenomen bij (potentiële) slachtoffers van mobile phishing naar beveiligingscodes van internetbankieren en semigestructureerde interviews worden afgenomen bij medewerkers van de bank. Voor het achterhalen van informatie bij (potentiële) slachtoffers worden online enquêtes afgenomen. Met behulp van enquêtes kan op een gestructureerde wijze in een korte tijd een groot aantal respondenten bereikt worden en kan verkregen informatie onderling met behulp van statistiek worden vergeleken. Semigestructureerde interviews worden afgenomen omdat het deels bekend is welke informatie opgevraagd moet worden bij een Nederlandse bank. Echter, omdat dit vervolgonderzoek exploratief van aard is zal naast gestructureerd interviewen ook ongestructureerd geïnterviewd worden om extra relevante informatie te verkrijgen.

3.2 Technisch ontwerp: uitwerking van de onderzoeksmethode(n)

In onderstaande tabel zijn de onderzoeksmethoden per deelvraag uitgewerkt.

Deelvraag	Onderzoeksmethode(n)
6. Wat doen de eindgebruikers van smartphones zelf ter beveiliging van hun beveiligingscodes voor internetbankieren?	**Enquête online afnemen:** Dichotome vraag in de enquête opnemen waarin gevraagd wordt of de smartphone is beveiligd tegen mobile phishing.
7. Welke oorzaken beïnvloeden slachtoffers om tijdens het gebruik van hun smartphone op een valse link te klikken en in te loggen met hun bankgegevens?	**Enquête online afnemen:** Multi select meerkeuzevraag in de enquête opnemen opgebouwd uit een lijst met aspecten die ervoor kunnen zorgen dat slachtoffers klikken op een phishing link. Ook de optie 'andere' aanbieden zodat een slachtoffer zelf een ander aspect kan opgeven.
8. In hoeverre zijn de maatregelen van banken om bankklanten te beschermen tegen mobile phishing naar beveiligingscodes voor internetbankieren bestand genoeg tegen mobile phishing naar beveiligingscodes voor internetbankieren?	**Semigestructureerde interviews afnemen:** exploratief onderzoek verrichten bij een bank om inzichtelijk te maken welke maatregelen banken tegen mobile phishing treffen, welke afdelingen zich hier mee bezig houden en hoe dit dagelijks in de werkzaamheden van betreffende bankmedewerkers wordt vormgegeven. Dit zal een mix zijn van gestructureerd en ongestructureerd interviewen. Er zullen twee bankmedewerkers semigestructureerd geïnterviewd worden. Hierbij zullen enkel open vragen worden gesteld. **Enquête online afnemen:** Dichotome vraag of de bestaande maatregelen van banken wel of niet bekend zijn bij de Nederlandse bevolking. Tevens met behulp van een 5 punts Likert schaal vragen in hoeverre deze maatregelen ertoe hebben geleid dat een potentieel slachtoffer niet trapt in een mobile phishing aanval. Respondenten kunnen bij een 5 punts

	likert schaal namelijk nuance aanbrengen en er is een midden voor als ze niet kunnen of willen kiezen.

Tot slot wordt in de enquête ook gebruik gemaakt van een 5 punts Likertschaal waarin de kwaliteit, volledigheid, bruikbaarheid en zinvolheid van de enquête wordt geëvalueerd.

De omvang van de populatie is onbekend. Als de populatiegrootte boven de 20.000 komt, zal de steekproefgrootte niet veel meer wijzigen. Vandaar dat de omvang van de steekproef 20.000 is. De populatie bevat mensen met een leeftijd tussen 17 en 99 jaar. Om een betrouwbaarheid van 95 % te garanderen dient de responsie minimaal 377 te bedragen. Dit aantal is als volgt bepaald:

Legenda

N = de populatie

Z = de Z-waarde van een normale distributie

P = de kans dat een bepaald antwoord wordt gegeven

Q = de kans dat een bepaald antwoord niet wordt gegeven

F = de foutmarge

$$Steekproef = \frac{\mathrm{N} * (\mathrm{z})^2 * \mathrm{P} * \mathrm{Q}}{\mathrm{z}^2 * \mathrm{P} * \mathrm{Q} + (\mathrm{N} - 1) * \mathrm{F}^2}$$

$$Steekproef\,(377) = \frac{20.000 * (1.96)^2 * 0.5 * (1 - 0.5)}{1.96^2 * 0.5 * (1 - 0.5). + (176.199) * 0.05^2}$$

Het 95-procent-betrouwbaarheidsinterval heeft een ondergrens van -4 % en +4% dus stel dat 80 % van de respondenten aangeeft de smartphone niet te beveiligen dan kan met een 95% zekerheid gezegd worden dat dit percentage in de gehele populatie zal liggen tussen de 76 % en 84 %. De berekening van de 95-procent- betrouwbaarheidsinterval is als volgt bepaald:

Onderstaande formule is gebruikt voor het berekenen van de 95-procent-betrouwbaarheidsinterval.

Vergelijking 1: Bron:https://www.thesishulp.nl/betrouwbaarheidsinterval-berekenen/

$$\hat{p} - z_{(alpha/2)} * \sqrt{\frac{\hat{p} * (1 - \hat{p})}{n}} < \bar{u} < p + z_{(alpha/2)} * \sqrt{\frac{\hat{p} * (1 - \hat{p})}{n}}$$

Berekening:

Ondergrens: 0.8- 1.96 x √ ((0.8*0,2)/377) =0.76

Bovengrens: 0.8+1.96 x √ ((0.8*0,2)/377) =0.84

Het surveyonderzoek dient te voldoen aan een aantal criteria. In de resultaten van de enquête dient zichtbaar te zijn dat respondenten van verschillende leeftijden tussen de 18 en 100 hebben deelgenomen. Daarnaast dienen deze respondenten allemaal een smartphone in bezit te hebben. Overigens dient er een mix te zijn van vrouwelijke en mannelijke respondenten en/ of respondenten met een ander geslacht om mogelijke patronen te kunnen ontdekken. Deze criteria zullen opgenomen worden in de enquête en gecorrespondeerd worden naar de respondenten.

3.3 Gegevensanalyse

Data wat met behulp van de enquêtes is verzameld wordt in Excel geanalyseerd door de verschillende antwoorden per vraag te vergelijken. Er zal gekeken worden naar hoeveel personen een bepaald antwoord hebben gegeven en of er patronen terug te vinden is in de antwoorden. Daarnaast zal er bijvoorbeeld gekeken worden welke antwoorden het meest, gemiddeld en het minst voorkomen.
De verkregen data van de enquêtes voor het beantwoorden van deelvraag 7 zal ook vergeleken worden met data verkregen vanuit de literatuur. Hierbij zal gekeken worden of dit onderzoek nieuwe aspecten bovenwater heeft gehaald die ertoe leiden dat een slachtoffer op een phishing link klikt.
De data verkregen van de semigestructureerde interviews zal geanalyseerd worden door de antwoorden van de geïnterviewden met elkaar te vergelijken. Verder zal de data wat is verkregen vanuit de semigestructureerde interviews vergeleken worden met data uit de literatuur om te beschrijven in hoeverre hiermee de literatuur wordt aangevuld.

3.4 Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Validiteit gaat over het vermogen van het meten wat men beoogt te meten (Saunders, Lewis & Thornhill, 2019, p. 213-214). Om de interne validiteit te waarborgen is eerst literatuuronderzoek gedaan en is inzichtelijk gemaakt welke informatie nog ontbreekt en deze informatie zal opgehaald worden vanuit interviews en enquêtes. De externe validiteit, de mate waarin de resultaten van dit onderzoek gegeneraliseerd kunnen worden buiten de onderzochte populatie is gewaarborgd door de enquêtes af te nemen bij respondenten uit de faceboekgroep ‘Fadim’s Beautyspace’ van verschillende leeftijden tussen de 16 en 48 jaar. Deze respondenten zijn actieve social mediagebruikers die een smartphone bezitten. Uit het literatuuronderzoek kwam namelijk naar voren dat mensen met een smartphone potentiële slachtoffers zijn voor mobile phishing naar beveiligingscodes voor internetbankieren. Om die redenen vormt de steekproef á 377 respondenten de juiste afspiegeling van de Nederlandse bevolking wat in bezit is van een smartphone. De externe validiteit van de interviews is laag omdat in dit onderzoek maar twee respondenten kunnen worden geïnterviewd.

Betrouwbaarheid gaat over de mate waarin een onderzoek herhaalbaar is en dezelfde uitkomsten oplevert (Saunders, Lewis & Thornhill, 2019, p. 213-214). Een valkuil in dit onderzoek is dat de respondenten de vragen anders interpreteren dan de onderzoeker heeft bedoeld. Om dit te beperken plaatst de onderzoeker zich in de respondenten en worden suggestieve en samengestelde vragen vermeden. In de interviews zullen de vragen vooraf gestuurd worden naar de geïnterviewden zodat van tevoren inzichtelijk is of de vragen duidelijk zijn. Na het afronden van de interviews zullen de antwoorden verstuurd worden naar de geïnterviewden om te checken of de antwoorden correct zijn.

De enquêtes en interviews zullen vrijwillig en anoniem worden afgenomen. Overigens zullen de interview gesprekken alleen opgenomen worden indien de twee geïnterviewden dit toestaan.

4. Resultaten

In dit hoofdstuk zijn de uitvoering van dit onderzoek en de resultaten beschreven.

4.1 Uitvoering onderzoek

4.1.1 Enquête

De populatie van de enquête betreft mensen uit de Nederlandse bevolking die in het bezit zijn van een smartphone en een online betaalrekening van een Nederlandse bank. Vooraf was het niet duidelijk hoeveel mensen in Nederland in het bezit zijn van een smartphone en een online betaalrekening. Vandaar dat de populatie onbekend is. Het oorspronkelijke plan was om de facebookgroep Fadim's Beautyspace als populatie te gebruiken. Echter is deze steekproef niet representatief genoeg voor de gehele Nederlandse bevolking. Daarnaast is de betreffende facebookgroep uit de lucht gegaan. Om die redenen is gekozen om het bereik te vergroten naar kennissen, verschillende facebookgroepen, Linkedin en Instagram bestaande uit mensen met een leeftijd tussen 17 en 99 jaar. Deze mensen zijn verspreid over heel Nederland. Zo kan het onderwerp via verschillende invalshoeken worden bekeken en wordt een beter beeld gevormd van de Nederlandse bevolking.
De enquête die is opgesteld bestaat uit 20 vragen. Een afdruk van deze enquête is terug te vinden in Bijlage 3. Met behulp van de enquête is informatie verzameld om deelvraag 6 tot en met 8 te beantwoorden. In hoofdstuk 3 is de steekproef beraamd op 377 respondenten om een betrouwbaarheid van 95 % te garanderen. Echter zijn slechts 198 respondenten verzameld die de enquête volledig hebben ingevuld. Daarnaast is de steekproef niet representatief omdat de gemiddelde leeftijd, gemiddeld aantal hoogopgeleiden, vrouwelijk geslacht niet overeenkomen met deze gemiddelden van de Nederlandse bevolking. Om deze reden zijn de resultaten van de enquête niet generaliseerbaar over de gehele populatie en dus niet significant. In de discussie (hoofdstuk 5) wordt hier verder op ingegaan.

4.1.2 Semigestructureerde interviews

Het was eigenlijk de bedoeling om semigestructureerde interviews af te nemen bij twee medewerkers die werkzaam zijn bij een ander van Nederlandse bank. Echter is het slechts gelukt om in contact te komen met één medewerker van slechts één Nederlandse bank. Er is gekozen om een medewerker te spreken die zich dagelijks bezighoudt met beveiligingsvraagstukken van de Nederlandse bank. Een Adviseur Fraud & Corporate Security heeft deelgenomen aan dit onderzoek. Naar deze medewerker zijn de interviewvragen per e-mail verstuurd en deze zijn per e-mail beantwoord. De reden waarom het gewenst was om medewerkers van meerdere Nederlandse banken te spreken is omdat de resultaten dan onderling met elkaar vergeleken konden worden en het onderwerp via verschillende invalshoeken bekeken kon worden. Daarnaast heeft ook geen interview plaatsgevonden en zijn gesprekken niet opgenomen. Echter, door het versturen van de vragenlijst zijn wel de juiste antwoorden verkregen en staat alles toch zwart op wit. De vragen en antwoorden zijn terug te vinden in Bijlage 4.

4.2 Resultaten

Hieronder zijn de resultaten weergegeven. Het plan voor de verwerking van de resultaten is terug te vinden in Bijlage 5.

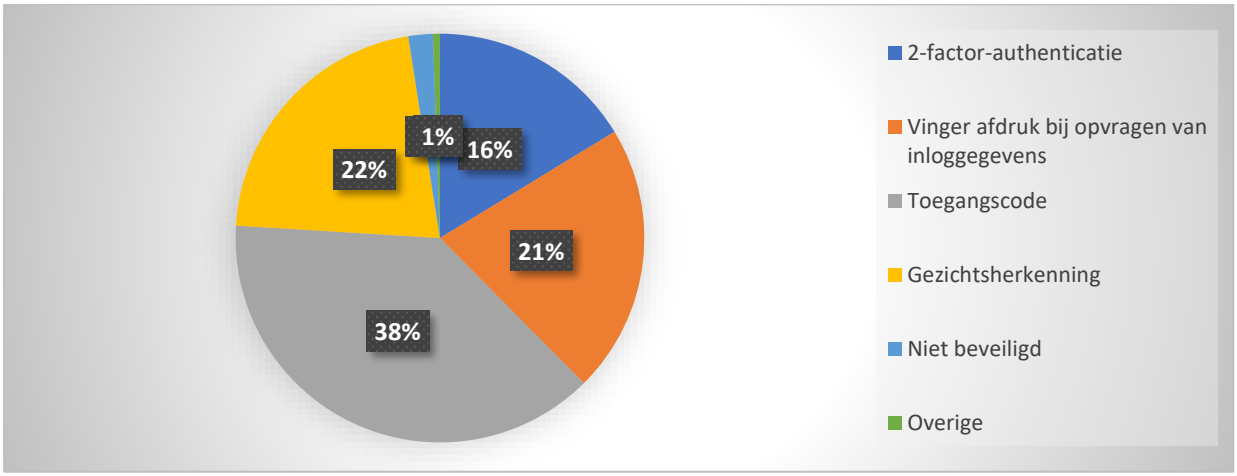
Als eerst wordt met de demografische factoren de kenmerken van de geënquêteerden beschreven. Zo blijkt dat de meeste geënquêteerden (67 procent) zich in de leeftijdsgroep van 21 tot 29 jaar bevinden. Bovendien is 63 procent vrouw en 37 procent man. Overigens is 64 procent hoogopgeleid. In *Tabel 2* worden de demografische factoren getoond.

Tabel 2: Beschrijvende statistiek- Demografische factoren

	Gemiddelde	Standaard deviatie
Leeftijd = 20 tot 29	0.67	0.24
Geslacht (1= vrouw)	0.63	0.31
Opleiding (1= hoogopgeleid)	0.64	0.10

Uit de demografische factoren blijkt al dat de steekproef niet representatief is voor de doelgroep. Het percentage jongeren (leeftijdsgroep 21-29), percentage geslacht vrouw en hoogopgeleiden is veel hoger dan een doorsnede uit de bevolking zou opleveren. Om die reden zijn de enquête resultaten niet generaliseerbaar naar de gehele populatie. In hoofdstuk 5 wordt hier verder op ingegaan.

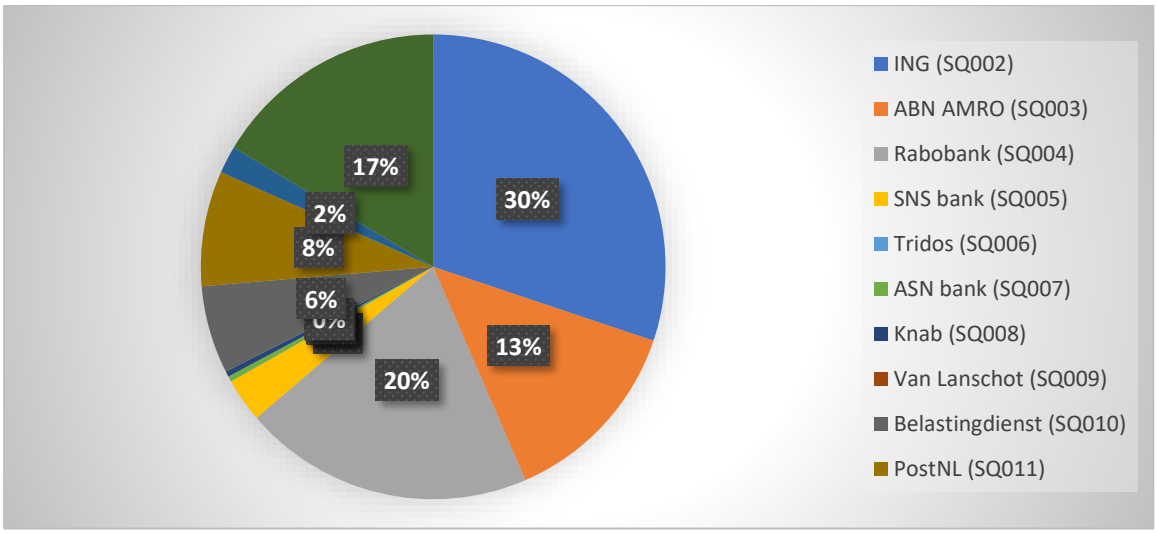
Nu wordt verder ingegaan op de beveiligingsmaatregelen die bankklanten treffen voor het beveiligen van alle inlogcodes van hun smartphone. In *Figuur 1* zijn de verschillende manieren weergegeven waarop de geënquêteerden hun smartphone beveiligen.



Figuur 1: Beveiligingsmaatregelen die geënquêteerden treffen voor inlogcodes smartphone

Uit *Figuur 1* is op te maken dat vier procent van de geënquêteerden de inlogcodes van de smartphone niet heeft beveiligd. De toegangscode wordt het meest gebruikt als beveiligingsmethode voor de inloggegevens van de smartphone. Slechts 16 procent van de geënquêteerden maakt gebruik van 2-factor-authenticatie. Momenteel is 2-factor-authenticatie de veiligste manier om de inloggegevens op de smartphone te beveiligen (Consumentenbond, 2021). Overigens is aan de geënquêteerden gevraagd of ze vinden dat hun smartphone voldoende beveiligd is tegen mobile phishing naar beveiligingscodes. Hieruit is naar voren gekomen dat 55 procent aangeeft dat de smartphone hier voldoende tegen beveiligd is en 45 procent geeft aan van niet. Het zou kunnen zijn dat de geënquêteerden hier denken dat het gaat om de beveiliging op het internet bankieren app, terwijl het eigenlijk gaat om de beveiliging van het inloggen op de bankomgeving via de mobiele webbrowser.

Voordat gekeken wordt naar de oorzaken waarom een slachtoffer op een valse link klinkt is onderzocht of de geënquêteerden überhaupt een phishing sms hebben ontvangen. Een phishing sms is een sms bericht die fraudeurs naar potentiële slachtoffers versturen en waarbij de fraudeurs zich valselijk voordoen als een Nederlandse bank of bekende instantie. Deze sms bericht bevat vaak een link waarin potentiële slachtoffers gevraagd worden om in te loggen met bankgegevens. 66 procent van de geënquêteerden geeft aan een phishing sms ontvangen te hebben van een Nederlandse bank of bekende instantie. In *Figuur 2* is de verdeling te zien van namens welke Nederlandse banken en instanties deze phishing sms is verstuurd.

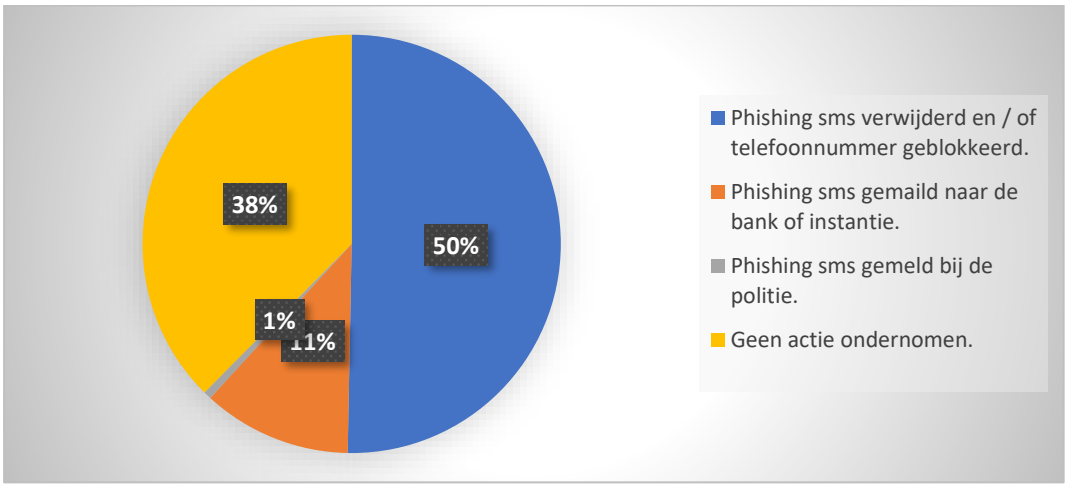


Figuur 2: Verdeling phishing sms-berichten namens banken en instanties

Uit *Figuur 2* is op te maken dat de meeste phishing sms'jes namens de ING-bank en daaropvolgend de Rabobank worden verstuurd. Onder overige hebben de geënquêteerden de volgende Nederlandse banken of instanties opgegeven: KBC, KPN, DHL en Visa.

De geënquêteerden is tevens gevraagd in welke periode ze een phishing sms hebben ontvangen. Zo blijkt dat in de periode 2020-2021 de meeste (61 procent) phishing sms-berichten werden verstuurd. In periode 2019-2020 ontving slechts 37 procent van de geënquêteerden een phishing sms. Dit is dus een stijging van 24 procent in één jaar tijd.

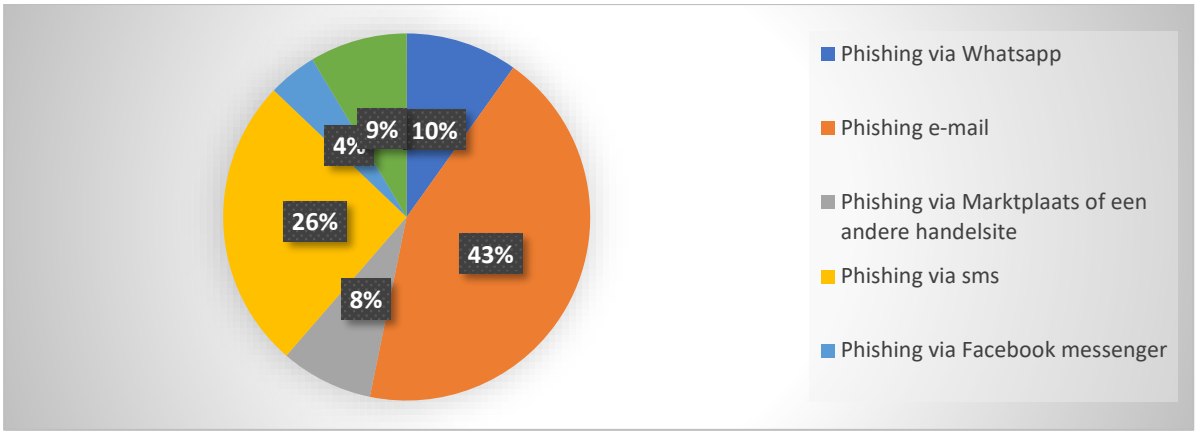
Nu zal verder ingegaan worden op de oorzaken waarom een potentieel slachtoffer op een phishing link klikt. Uit de enquête is gebleken dat slechts drie van de 198 geënquêteerden op de phishing link van het phishing sms-bericht hebben geklikt. Oorzaken die hiervoor worden aangeduid zijn dat ze niet bekend waren met het feit dat er phishing sms-berichten worden verstuurd, ze de link niet hebben gecheckt omdat de link op de webbrowser van smartphone niet geheel wordt weergegeven en omdat ze geen waarschuwing op hun smartphone kregen dat het om een valse website ging. In *Figuur 3* is de verdeling van de acties weergegeven die de geënquêteerden hebben ondernomen na het ontvangst van een phishing sms-bericht.



Figuur 3: Getroffen acties na ontvangst van een phishing sms

Uit *Figuur 3* is op te maken dat de 50 procent van de geënquêteerden de phishing sms verwijdert en / of telefoonnummer van het phishing sms blokkeert. Maar in *Figuur 4* valt op dat maar liefst 38 procent geen actie onderneemt na het ontvangen van een sms-bericht.

Overigens is aan de geënquêteerden gevraagd met welke andere vormen van phishing naast mobile phishing ze te maken hebben gehad. In *Figuur 4* zijn de resultaten hiervan weergegeven.



Figuur 4: Verdeling diverse soorten phishing aanvallen

Uit *Figuur 4* is op te maken dat phishing via e-mail het vaakst voorkomt (43 procent), gevolgd door phishing via de sms (28 procent). De geënquêteerden hebben de volgende voorbeelden van phishing gemeld:

- Phishing via facebook Messenger: ''Een geautomatiseerd bericht van een vriend of vriendin met: ''Ik heb 100.000 euro gewonnen door..''''
- Phishing via whatsapp: ''Iemands account was gehackt en moest geld lenen.''
- Via de e-mail: ''Bol.com cadeaukaarten door te klikken op een link'', ''mail van Apple dat er nog een rekening open staat'', ''een mail van dat je je creditcardgegevens moet invullen of in moet loggen op een crypto account'', ''e-mails namens bedrijven door fraudeurs'.'
- Phishing via de sms: ''Nieuwe betaalpas aanvragen'', ''PostNL''.

De frequentie waarin de geënquêteerden te maken hebben gehad met dergelijke vormen van phishing verschilt van 1 tot 20 keer, dagelijks, maandelijks tot eens per jaar.

Voordat wordt ingegaan op de maatregelen die banken treffen om mobile phishing tegen te gaan wordt eerst beschreven welke gevolgen gepaard gaan met deze vorm van phishing. De respondent van een Nederlandse bank gaf aan dat deze vorm van phishing veelal financiële gevolgen heeft. In sommige gevallen lukt het de fraudeur namelijk om daadwerkelijk geld van de klant af te nemen. Situatie afhankelijk kan dit betekenen dat deze schade door de Nederlandse bank wordt vergoed. Aanvullend hierop hebben de drie slachtoffers die geënquêteerd zijn de volgende financiële- en geestelijke gevolgen opgegeven: verlies van geld, pijn, verlies van vertrouwen en boosheid. Financieel gezien hebben deze drie getroffen geënquêteerden afzonderlijk tussen de 500 en 1.000 euro verloren aan mobile phishing naar beveiligingscodes voor internetbankieren.

Als gevolg van de financiële gevolgen van zowel de bank als de slachtoffers probeert de betreffende Nederlandse bank te voorkomen dat klanten slachtoffer worden van onder andere mobile phishing. Nederlandse banken hebben namelijk een zorgplicht tegenover de klanten waar de betreffende Nederlandse bank zo goed mogelijk aan wil voldoen. De respondent van de Nederlandse bank gaf aan dat de Nederlandse bank de klanten via verschillende communicatiekanalen waarschuwt om niet te

reageren op phishingmails/sms'jes. Bij de verschillende communicatiekanalen kan men denken aan de website van de bank, Twitter en op de internet bankieren app. Banken creëren herhaaldelijk bewustwording bij de klanten door klanten op de website van informatie te voorzien en klanten krijgen regelmatig waarschuwingen pop-ups wanneer ze willen internetbankieren. De respondent gaf ook aan dat er een samenwerking is tussen de banken onderling om bijvoorbeeld middels commercials op tv aandacht te schenken aan dit onderwerp. Naast het waarschuwen van klanten worden klanten ook via de website van de bank voorzien van tips waaraan ze een phishing bericht kunnen herkennen. De fraudeafdeling van de Nederlandse bank houdt zich dagelijks bezig met het bijhouden van wat de trends van deze vorm van fraude zijn. Hoe meer de fraudeafdeling van de Nederlandse bank inzake de wijze waarop de fraudeurs te werk gaat hoe meer gericht de Nederlandse bank hierop kan acteren. De Nederlandse bank heeft een specifieke fraudeafdeling die hier dagelijks actief mee bezig is. Er zijn diverse werkzaamheden die gericht zijn op de fase nadat een fraude heeft plaatsgevonden. Maar een gedeelte van de afdeling houdt zich ook actief bezig met het voorkomen van fraudes zoals mobile phishing naar beveiligingscodes voor internetbankieren. Zo blijkt dat er bijvoorbeeld een detectiesysteem wordt gebruikt die mogelijk frauduleuze transacties tijdig kan herkennen en op deze wijze is het vaak ook mogelijk om de schade tijdig te voorkomen. Over de ins en outs van dit systeem kon de respondent niet veel bekend maken.

Er is tenslotte aan de respondent van de Nederlandse bank gevraagd hoe effectief deze getroffen maatregelen volgens de Nederlandse bank zijn. Ondanks de maatregelen die de bank treft komt de betreffende vorm van mobile phishing nog steeds landelijk in grote mate voor. Ondanks dat banken veel aandacht besteden aan de communicatie naar de bankklanten middels diverse kanalen zijn er namelijk nog mensen die een betreffende fraudepoging niet tijdig herkennen en daadwerkelijk gaan inloggen met hun bankgegevens. Volgens de respondent draagt communicatie wel degelijk bij en zorgt het ervoor dat bankklanten sneller bewust worden gemaakt. Volgens de respondent zal er helaas altijd een groep mensen zijn die ondanks de communicatie de betreffende fraudepoging toch niet herkennen en zodoende niet tijdig in kunnen grijpen. Daarnaast draagt het detectiesysteem goed bij aan het tijdig detecteren van frauduleuze transacties. De respondent geeft aan dat dagelijks een gedeelte van de verdachte frauduleuze transacties tijdig worden gestopt, zodat schade wordt voorkomen. Ook hierbij geld dat er een groot aantal frauduleuze transacties helaas niet tijdig gestopt kunnen worden.

5. Conclusies, discussie en aanbevelingen

5.1 Conclusies

De volgende onderzoeksvraag stond centraal in dit onderzoek: *Wat moet er in Nederland gebeuren om mobile phishing naar beveiligingscodes voor internetbankieren tegen te gaan?*

Uit zowel het literatuur- als het empirisch onderzoek is naar voren gekomen dat mobile phishing naar beveiligingscodes voor internetbankieren een steeds groeiend probleem is in Nederland. Zo blijkt uit het onderzoek van Roks en Monshouwer (2020) dat criminelen op online platform 'Telegram' pakketten aanbieden voor het plegen van mobile phishing aanvallen. Dit biedt iedereen, zelfs mensen met weinig technische kennis, de mogelijkheid om zelf mobile phishing aanvallen te plegen. Kenmerkend is dat ondanks dat dit probleem steeds meer groeit er weinig onderzoek is gedaan naar dit probleem. Zo blijkt dat het proces van mobile phishing in voorgaande onderzoeken niet geheel in kaart is gebracht en dat het niet duidelijk is in hoeverre de Nederlandse bevolking zich bewust is van dit probleem. Ook is het precieze aantal en toename in mobile phishing naar beveiligingscodes voor internetbankieren in Nederland niet bekend.

Ook kwam uit het literatuuronderzoek niet naar voren welke maatregelen banken precies treffen om mobile phishing tegen te gaan en hoe effectief deze maatregelen zijn. Alhoewel uit het literatuuronderzoek kwam naar voren dat Nederlandse banken voorlichtingscampagnes geven aan klanten en klanten waarschuwen op hun website. Het empirisch onderzoek bevestigt dit aanvullend met dat detectiesystemen worden gebruikt om frauduleuze transacties tijdig tegen te houden of te beperken. Ook kwam uit het empirisch onderzoek naar voren dat klanten regelmatig waarschuwingen pop-ups krijgen wanneer ze willen internetbankieren. Aangenomen wordt dat de maatregelen die banken dagelijks treffen wel degelijk bijdragen aan het terugdringen van slachtoffers van deze vorm van phishing. Alleen is dit niet cijfermatig aan te tonen omdat niet bekend is hoeveel frauduleuze transacties met betrekking tot mobile phishing worden tegengehouden. Ook is niet bekend hoeveel mensen na het ontvangen van een waarschuwing niet ingaan op de phishing sms-berichten.

Onderzoekers beperken zich tot financiële gevolgen van mobile phishing naar beveiligingsbankieren. Echter, uit het empirisch onderzoek is ook naar voren gekomen dat slachtoffers geestelijke gevolgen ervaren door mobile phishing naar beveiligingscodes van internetbankieren. Hierbij kan men denken aan pijn, verdriet en verlies van vertrouwen.

Daarnaast is uit het empirisch onderzoek naar voren gekomen dat de Nederlandse bevolking ook maatregelen treft om inloggegevens van hun smartphone te beveiligen. Echter kwam uit het literatuuronderzoek al naar voren dat deze maatregelen niet bestand zijn tegen mobile phishing omdat mobile phishing plaatsvindt op de webbrowser. Er zijn geen technieken ontwikkeld waarmee klanten gewaarschuwd worden dat ze via de webbrowser inloggen op een phishing website. Overigens is uit het literatuuronderzoek naar voren gekomen dat onderzoekers zich hebben beperkt tot een aantal redenen waarom smartphone gebruikers het belangrijkste doelwit zijn van phishing aanvallen: kleine scherm op smartphone, onvoldoende beveiliging webbrowser en onvoldoende bewustwording mobile phishing. Het empirisch onderzoek bevestigd dat slachtoffers om bovengenoemde redenen op de phishing link klikken.

Het antwoord op de onderzoeksvraag is dat dit probleem aangepakt kan worden door als eerst meer onderzoek te verrichten naar het proces van mobile phishing en naar hoe de verspreiding van mobile phishing pakketten tegengegaan kan worden. Daarnaast dienen Nederlandse banken verder te onderzoeken hoe de online betaalomgeving via de webbrowser beter beveiligd kunnen door

bijvoorbeeld extra verificatievragen toe te passen bij het inloggen of 2 factorauthenticatie toe te passen. Ook dient er een beveiligingsmethode ontwikkeld te worden waardoor potentiële slachtoffers direct gewaarschuwd worden dat het om een phishing website gaat en ze niet moeten inloggen met hun bankgegevens.

5.2 Discussie – reflectie

5.2.1 Literatuuronderzoek

Het literatuuronderzoek is uitgevoerd door zoekmachine Summon en Google Scholar te gebruiken. Naast het raadplegen van Google Scholar en de zoekmachine Summon is via Google recente informatie opgezocht van RTL-nieuwberichten, Nederlandse betaalvereniging en de fraudehelpdesk. Ondanks het feit dat Summon, Google Scholar en google gebruikt zijn voor het vinden van artikelen en nieuwsberichten rest de mogelijkheid dat dat relevante literatuur is gemist en dus niet is opgenomen in dit onderzoek. Uit het literatuuronderzoek kwam niet naar voren hoe de Nederlandse bevolking kijkt naar het probleem mobile phishing naar beveiligingscodes voor internetbankieren in Nederland. Ook was niet duidelijk welke maatregelen banken treffen om dit probleem tegen te gaan. Daarnaast was het uit de literatuur te achterhalen met welke gevolgen naast financiële gevolgen slachtoffers van mobile phishing nog meer kampen. Om die reden zijn bovengenoemde aspecten verder onderzocht in het empirisch onderzoek.

Desalniettemin is in de literatuur wel relevante informatie gevonden waarmee onder andere het proces van mobile phishing in kaart is gebracht en mogelijke oorzaken van het succes van een mobile phishing aanval zijn beschreven. Ook is uit literatuur naar voren gekomen dat mobile phishing een steeds groeiend probleem is in Nederland en dat het vrij eenvoudig is om als Nederlands burger zelf een mobile phishing aanval te plegen. In het empirisch onderzoek is daarom verder onderzocht in hoeverre mobile phishing is toegenomen in de periode 2018 tot 2021. Een deel van de resultaten uit dit onderzoek komt overeen met inzichten uit bestaand wetenschappelijk onderzoek. Zo blijkt dat het aantal phishing aanvallen inderdaad de afgelopen jaren (2018-2021) zijn toegenomen. Ook de bevinding dat de Nederlandse bank die betrokken was in dit onderzoek via diverse communicatiekanalen bankklanten waarschuwen voor phishing klopt. Dat zowel banken als slachtoffers van mobile phishing financiële gevolgen ervaren klopt ook.

5.2.2 Empirisch onderzoek

De enquête resultaten uit het empirisch onderzoek zijn niet significant. Allereerst is de samplegrootte niet gehaald omdat slechts 198 respondenten de enquête volledig hebben ingevuld. De sample moest 377 respondenten bevatten om een betrouwbaarheid van 95 % te garanderen. Daarnaast is de steekproef niet representatief voor de Nederlandse bevolking om de volgende redenen. Uit de databank CBS is naar voren gekomen dat 50,4 procent van de Nederlandse bevolking een vrouwelijk geslacht heeft (CBS, 2020). In dit onderzoek bedraagt het percentage vrouw 63 procent. Daarnaast bedraagt volgend het CBS het percentage hoogopgeleiden uit Nederland (HBO/ WO) 32,2 procent (CBS,2020). Terwijl het percentage hoogopgeleiden in dit onderzoek 64 procent bedraagt. Overigens bevonden de meeste respondenten zich in de leeftijdsgroep van 21-29 terwijl de gemiddelde leeftijd van Nederlanders 42,2 jaar bedraagt (CBS, 2020). Oorzaken hiervoor kunnen zijn dat de enquête veelal is verspreid onder mijn netwerk wat veelal uit hoogopgeleide vrouwen bestaat met een leeftijd tussen de 21 en 29 jaar. Verder zijn respondenten vergaard door leden uit mijn netwerk de enquête te laten delen. Waarschijnlijk zijn kennissen van mijn netwerk ook grotendeels hoogopgeleid en vrouw en behoren ze ook tot de leeftijdsgroep 21-29 jaar. Hierdoor is de steekproef niet helemaal representatief. Dus zelfs als de minimale sampelgrootte wel gehaald was zouden de resultaten niet generaliseerbaar zijn naar de gehele populatie.

In de introductie van de enquête is het doel van dit onderzoek duidelijk beschreven. Echter ontbreekt de definitie van mobile phishing in de introductie. De vraag is of alle geënquêteerden bekend zijn met

de term ‘mobile phishing’ en meteen snappen waarover de enquête gaat. Echter is de definitie van mobile phishing wel opgenomen in de vragenlijst van de enquête en is deze zelfs geïllustreerd met een afbeelding.

Ook de vraagstelling wat is opgenomen in de enquête over op welke manier de inlog gegevens van de smartphone van slachtoffers zijn beveiligd had eigenlijk anders gesteld moeten worden. Er had gevraagd moeten worden op welke manier de inloggegevens van internetbankieren via de webbrowser zijn beveiligd. Dan was het duidelijker geweest in hoeverre deze inloggegevens op de webbrowser zijn beveiligd in plaats van op de bankieren app. Nu is het namelijk de vraag of de geënquêteerden het zo hebben geïnterpreteerd.

Nederland heeft sinds het jaar 2020 te maken met het coronavirus (COVID19). Wat betreft de dataverzameling middels een enquête heeft dit geen negatieve invloed gehad. Data is verzameld middels een online vragenlijst wat is opgesteld in Limesurvey. Echter, wordt aangenomen dat COVID19 wel een negatieve invloed heeft gehad op de dataverzameling middels semigestructureerde interviews met medewerkers van Nederlandse banken. De reden hiervan is omdat het slechts gelukt is om één relevante medewerker van één Nederlandse bank een vragenlijst te mailen. Dus een echt interview heeft niet plaats gevonden. Bij andere banken is de vraag ook meerdere maak uitgezet om een semigestructureerd interview te houden met een betreffende medewerker van de bank. Echter in de meeste gevallen is geen reactie ontvangen of was er geen tijd voor een semigestructureerd interview. Dus dit is overmacht en daar was verder geen invloed meer op uit te oefenen.

5.3 Aanbevelingen voor de praktijk

Aanbevolen wordt dat de politie dit probleem meer prioriteit geeft door bijvoorbeeld in kaart te brengen op welke online platformen mobile phishing pakketten worden aangeboden. Uit zowel literatuur-als empirisch onderzoek kwam namelijk naar voren dat dit probleem steeds meer aan het groeien is in Nederland. Dit komt mede omdat het zo eenvoudig is om aan een mobile phishing pakket te komen en dus een mobile phishing aanval te plegen. Bovendien wordt aanbevolen om nog meer bewustwording onder de Nederlandse bevolking te creëren door bijvoorbeeld commercials op tv of kranten. Zo wordt ook bewustwording gecreëerd onder 65-plussers. Uit de cijfers van het CBS blijkt namelijk dat 65-plussers meer tv kijken dan 15-64-jarigen (CBS, 2021). Deze groep mensen zijn vaak de zwakste schakel en de kans is groter dat ze slachtoffer worden door gebrek aan kennis en bewustwording.

5.4 Aanbevelingen voor verder onderzoek

Allereerst wordt aanbevolen om een soortgelijk onderzoek te herhalen en daarbij slachtoffers van mobile phishing te enquêteren. Dan kan bijvoorbeeld onderzocht worden of er een verband is tussen demografische factoren en het slachtofferschap van mobile phishing. Ook zouden dan eventueel meer redenen boven water komen van waarom slachtoffers op de phishing link klikken en via de webbrowser inloggen met hun bankgegevens. Tevens dient onderzoek gedaan te worden naar een technologie om phishing websites meteen te detecteren en potentiële slachtoffers een melding geven dat het om een phishing website gaat. Voorgaande onderzoeken over phishing detectie technologieën gaan namelijk niet in op het waarschuwen van potentiële slachtoffers door middel van bijvoorbeeld een pop up . Daarnaast dient verder onderzocht te worden welke maatregelen de Nederlandse politie precies treft en verder kan treffen om mobile phishing tegen te gaan. Ook dient onderzocht te worden hoe inloggegevens voor internetbankieren bij alle Nederlandse banken beter beveiligd kunnen worden door bijvoorbeeld 2 factor authenticatie in te bouwen in het online bankieren website omgeving.

Literatuurlijst

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. Computers & Security, 68, 160–196.

Avrotros. (08-10-2019). Sms-bericht van 'ING' kun je rustig negeren. Geraadpleegd op 15-11-2020 van: https://opgelicht.avrotros.nl/alerts/artikel/sms-bericht-van-ing-kun-je-rustig-negeren/

Betaalvereniging Nederland. (2020). Geraadpleegd op 12-11-2020 van: https://www.betaalvereniging.nl/veiligheid/fraudecijfers/

Bojjagani, S., Brabin, D. R. D., & Rao, P. V. V. (2020). PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification. Procedia Computer Science, 171, 1110–1119.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors: The Journal of the Human Factors and Ergonomics Society, 58(8), 1198–1172.

CBS, Statline, bevolking; kerncijfers. Geraadpleegd op 03-04-2021 van https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37296ned/table?fromstatweb

Consumentenbond. (01-03-2021). Tweefactorauthenticatie activeren. Geraadpleegt op 08-04-2021 van https://www.consumentenbond.nl/veilig-internetten/activeer-tweestaps-authenticatie?fbclid=IwAR3WSczUi-GkRfyW6Woj9_n8GW46_IdX8HLL3rxCW-_26l-BjpUSebEE4_g

Van Dijke, W. RTL-nieuws (2019,26 november) 'Grote toename phishing via WhatsApp' (nieuws artikel). Geraadpleegd op 20-9-2020 van: https://www.rtlnieuws.nl/tech/artikel/4934691/whatsapp-phishing-linkje-marktplaats-speurders-sms-bankpas-betalen

Van Dijke, W. RTL-nieuws (2020, 19 juni) 'Internetoplichting explodeert door corona, minder inbrekers en zakkenrollers' (nieuws artikel). Geraadpleegd op 20-9-2020 van: https://www.rtlnieuws.nl/tech/artikel/5159956/cybercrime-fraude-corona-misdaad-inbraak-zakkenrollen-politie

E, M., & A, K. (2019). New Authentication Scheme to Secure against the Phishing Attack in the Mobile Cloud Computing. Security and Communication Networks, 2019, 1–11.

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security, 73, 519–544.

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2016). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28(12), 3629–3654.

Jaarrekening Stichting Aanpak Financieel- Economische Criminaliteit in Nederland. (2019). Boom register accountants.

Kadhim, H. Y., Al-saed, K. H. (2019). Mobile Phishing Websites Detection and Prevention Using Data Mining Techniques. International Journal of Interactive Mobile Technologies. 13(10), 205-213

Khonji, M., Iraqi, Y., Jones, A. (2013). Phishing detection: a literature survey. IEEE Commun Surveys Tutor, 15 (4), 2091-2121.

Kumar, S., Faizan, A., Viinikainen, A., Hamalainen, T. (2018). MLSPD - Machine Learning Based Spam and Phishing Detection. Computational Data and Social Networks, 510-522.

Odeh, A., Alarbi, A., Keshta, I., Abdelfattah, E. (2020). Efficient prediction of phishing websites using multilayer perceptron. Journal of Theoretical and Applied Information Technology. 98(6), 3353-3363.

Politie. Phishing. Geraadpleegd op 13-11-2020 van: https://www.politie.nl/themas/phishing.html#alinea-title-phishing-naar-inloggegevens

Roks, R., Monshouwer, N. (2020). F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger Justitiële verkenningen. 46(2), 44-58

Rooyakkers, J., Kranenbarg, M.W. (2020). Vissen met een nieuwe hengel: een onderzoek naar betaalverzoekfraude. Justitiele verkenningen. 46(2), 19-43

Saunders, Lewis, & Thornhill. (2019). Methoden en technieken van onderzoek (8e ed.). Amsterdam, Nederland: Pearson Benelux.

Shahriar, H., Zhang, C., Dunn, S., Bronte, R., Sahlan, A., & Tarmissi, K. (2019). Mobile anti-phishing: Approaches and challenges. Information Security Journal: A Global Perspective, 28(6), 178–193.

Shahriar, H., Klintic, T., Clincy, V. (2015). "Mobile Phishing Attacks and Mitigation Techniques", in Journal of Information Security.6, 206-212.

Veilig bankieren. (2020). Geraadpleegd op 15-11-2020 van: https://www.veiligbankieren.nl/

Verkijika, S.F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender''. Computers in Human Behavior. *101*,28-296.

Vijayalakshmi, M., Mercy Shalinie, S., Yang, M. H., & U., R. M. (2020). Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions. IET Networks, 9(5), 235–246.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586.

Van Wegberg, R., Tajalizadehkhoob, S. (2018). 'Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets', in: Proceedings of the 27th USENIX Security Symposium, Baltimore: USENIX 2018, 1009-1026.

Bijlage 1: Gedefinieerde parameters literatuuronderzoek

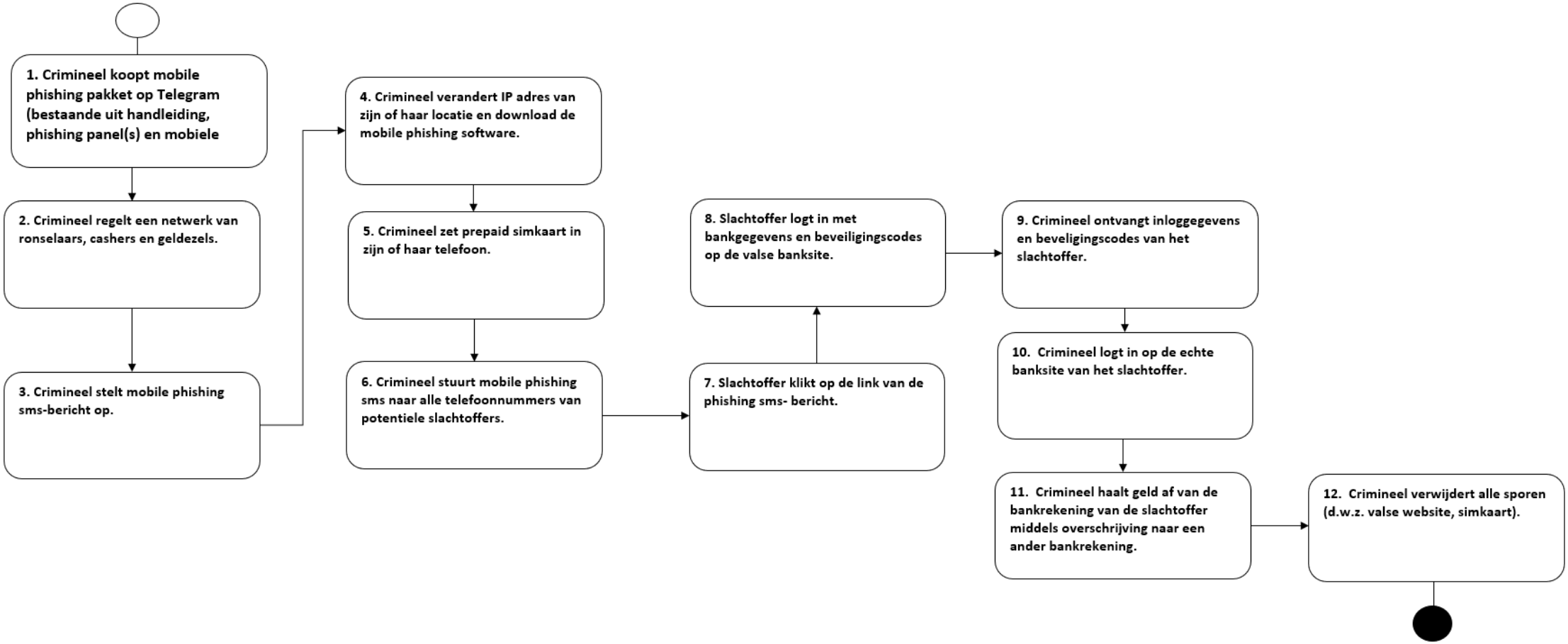
Taal: Engels en Nederlands

Periode : 2000 tot 2021

Type bronnen: vakliteratuur, wetenschappelijke artikelen, universitair afstudeeronderzoeken, krantenartikelen, nieuwsberichten, website instanties zoals de politie, Nederlandse banken of fraudehelpdesk.

Bijlage 2: Proces mobile phishing naar beveiligingscodes voor internetbankieren

Uit onderzoek van Roks en Monshouwer (2020) is naar voren gekomen dat criminelen op online platform 'Telegram' pakketten aanbieden voor het plegen van mobile phishing aanvallen. Dit biedt iedereen, zelfs mensen met weinig technische kennis, de mogelijkheid om zelf mobile phishing aanvallen te plegen. De mobile phishing pakketten bevatten een gebruikersvriendelijke handleiding, een lijst met mobile nummers van potentiële slachtoffers en een phishing panel. Op de website van de politie (2020) van Nederland is beschreven dat door een phishing panel een slachtoffer via het klikken op een valse link uitkomt bij de valse site van de bank. De handleiding voor het plegen van een mobile phishing aanval bevat een uitgebreide en stapsgewijze beschrijving voor het succesvol plegen van een mobile phishing aanval naar beveiligingscodes voor internetbankieren (Roks & Monshouwer, 2020, blz. 44-58) (van Wegberg & Tajalizadehkhoob, 2018, blz. 1009-1026). Met zulke gebruiksvriendelijke tools die beschikbaar worden gemaakt op Telegram, kunnen dergelijke aankopen van mobile phishing pakketten leiden tot een ongekende explosie van mobile phishing aanvallen. Op de website van de politie staat dat het plegen van phishing over het algemeen zeer laagdrempelig is: 'heb je een panel, een netwerk van ronselaars, cashers en geldezels, dan kun je aan de slag'. In *Afbeelding 1 (volgende pagina)* is het gehele proces van een mobile phishing aanval weergegeven.



Afbeelding 1:Proces mobile phishing aanval naar beveiligingscodes van internetbankieren.

Na het ontvangen van een mobile phishing pakket stelt de crimineel een mobile phishing sms-bericht op. De crimineel kopieert en plakt de tekst in een leeg sms-bericht (inclusief de illegitieme link naar de valse bankwebsite) uit de verkregen handleiding. Vervolgens plaatst de crimineel een prepaid simkaart in zijn of haar mobiele telefoon. De reden waarom prepaid-simkaarten worden gebruikt voor het plegen van mobile phishing aanvallen is omdat hiermee de identiteit van de crimineel niet achterhaald kan worden. De naam van de crimineel en adresgegevens blijven namelijk anoniem bij het gebruik van een prepaid-simkaart. Daarnaast verandert de crimineel volgens instructie het IP-adres om onvindbaar te blijven en de illegale mobile phishing software te kunnen downloaden (Roks & Monshouwer,2020, blz. 44-58). Hierdoor is het lastig voor de politie om de criminelen van mobile phishing aanvallen op te sporen. De volgende stap betreft het versturen van een phishing sms naar alle mobiele nummers van potentiële slachtoffers. In *Afbeelding 2* is voorbeeld van een phishing sms-bericht weergegeven die naar potentiële slachtoffers wordt verstuurd.

Afbeelding 2: Voorbeeld phishing sms-bericht met hierin een illegitieme URL van een valse ING-website (Avrotros, 2020)

In *Afbeelding 2* is te zien dat het phishing sms-bericht wordt verstuurd door een 06-nummer. Dit zijn dus nummers van prepaid simkaarten die de criminelen gebruiken om mobile phishing aanvallen anoniem te kunnen plegen. Bovendien is in *Afbeelding 1* te zien dat de phishing sms-berichten een link bevatten wat potentiële slachtoffers leidt naar een valse website wat identiek is aan de website van een bank (zie *Afbeelding 3*). Op deze manier worden slachtoffers misleid om met hun bankgegevens in te loggen (Choudhary & Jain, 2017, blz. 349) (Aleroud & Zhou, 2017, blz 160) (Goel & Jain, 2018, blz. 519-520) (Munivel & Kannammal, 2019, blz. 1939-2014) (Rooyakkers & Kranenbarg, 2020, blz. 19-43) (E.M. & A.K., 2019, blz.1-11) (Verkijika,2019, blz. 28-296).

Afbeelding 3: Voorbeeld valse illegitieme website ING (Avrotros,2019)

Vervolgens loggen slachtoffers met hun bankgegevens en beveiligingscodes in op de valse banksite. Nadat een slachtoffer is ingelogd op de valse banksite, zien de cyber criminelen het door de slachtoffer

ingevoerde gegevens. Deze gegevens worden met behulp van de illegale mobile phishing software vanuit de achterkant van de valse website achterhaald. Vervolgens loggen de cyber criminelen in op de echte banksite van het slachtoffer (Rooyakkers & Kranenbarg, 2020, blz. 19-43) (Politie, 2020). De criminelen halen het geld van de rekening van de slachtoffers af en pinnen het geld dan zo snel mogelijk uit een betaalautomaat (Roks & Monshouwer, 2020, blz. 44-58). De allerlaatste stap betreft het verwijderen van de valse bankwebsite, de simkaart en andere sporen van de mobile phishing aanval. In het onderzoek van Gupta et al (2017) is beweerd dat criminelen ook de mate van succes van hun mobile phishing aanvallen meten om toekomstige aanvallen te verbeteren.

Bijlage 3: Enquête: Onderzoek mobile phishing naar beveiligingscodes voor internetbankieren.

De onderzoeksgegevens zullen worden gebruikt voor onderzoek dat wordt uitgevoerd aan de Open Universiteit, waar wordt onderzocht wat er moet gebeuren om mobile phishing naar beveiligingscodes voor internetbankieren in Nederland te voorkomen. Deze vorm van mobile phishing is een probleem in Nederland wat nu in tijden van Corona steeds vaker voorkomt. Hierdoor worden slachtoffers die op de phishing link klikken en inloggen met hun bankgegevens zwaar getroffen. Het doel van deze enquête is om inzicht te krijgen in dit probleem vanuit de perspectief van de Nederlandse bevolking en achterhalen welke motieven slachtoffers hebben om met hun bankgegevens op de valse website in te loggen.

Desgewenst kunt u een kopie van het resulterende rapport ontvangen. Hiervoor word je aan het begin van de enquête uitgenodigd om een e-mailadres in te vullen. Dit adres wordt apart van de andere reacties opgeslagen, wordt alleen gebruikt om je een kopie van het onderzoeksrapport te mailen en wordt daarna direct verwijderd. Onderzoeker Linda Bujitu voert dit onderzoek uit en is te bereiken via mobile-security@ou.nl

Sommige gegevens met betrekking tot jou worden verzameld als je akkoord gaat met deelname. Deze worden alleen voor dit onderzoeksproject gebruikt. Op het moment van publicatie van de onderzoeksresultaten worden gegevens anoniem door alle persoonsgegevens te verwijderen die tot jou herleidbaar zijn.

- Ik verklaar dat ik duidelijk ben geïnformeerd over de aard, de methode en het doel van het onderzoek Gedacht over mijn deelname aan dit onderzoek Ik begrijp dat ik bij deelname aan het onderzoek mijn medewerking op elk moment en zonder opgaaf van redenen kan stopzetten.
- Door verder te gaan bevestig ik de bovenstaande uitspraken en mijn deelname aan dit onderzoek.

Vraag 1: Wat is je e-mailadres?

Vraag 2: Wat is je leeftijd?

- Jonger dan 18 jaar
- 18-20 jaar
- 21-29 jaar
- 50-59 jaar
- Ouder dan 59 jaar

Vraag 3: Wat is je geslacht?

- Man
- Vrouw
- Anders

Vraag 4: In welke provincie woon je?

- Friesland
- Groningen
- Drenthe
- Overijssel

- Flevoland
- Gelderland
- Utrecht
- Noord-Holland
- Zuid-Holland
- Zeeland
- Noord-Brabant
- Limburg

Vraag 5: Wat is je hoogst behaalde opleiding?

- Geen opleiding
- HAVO/ VWO
- VMBO
- MBO
- HBO Bachelor
- HBO Master
- Universiteit Bachelor
- Universiteit Master
- Universiteit Doctor

Vraag 6: Bij welke Nederlandse bank(en) heb je een bankrekening?

- ING
- ABN Amro
- Rabobank
- BUNQ
- ASN Bank
- SNS Bank
- Knab
- Anders, namelijk:

Vraag 7: Een phishing sms is een valse sms waarin een crimineel zich voordoet als een Nederlandse bank zoals de ING-bank, Rabobank of een andere bekende instantie zoals de Belastingdienst en verleid om middels een valse link in te loggen in jouw online bankomgeving.

Vraag 8: Heb je ooit een soortgelijk phishing sms ontvangen?

- Ja
- Nee

Vraag 9: Met welke andere vormen van phishing heb je te maken gehad?

- Phishing via Whatsapp
- Phishing e-mail
- Phishing via Marktplaats

Vraag 9: Namens welke bank of instantie werd deze phishing sms verstuurd?

- ING
- ABN AMRO
- Rabobank
- SNS bank
- Tridos
- ASN bank
- Knab
- Van Lanschot
- Belastingdienst
- PostNL
- T-Mobile
- Anders, namelijk:

Vraag 10: In welke periode(s) heb je een phishing sms ontvangen?

- Eerder dan 2018
- 2018-2019
- 2020-2021
- 2021-2022

Vraag 11: Hoe vaak heb je een phishing sms ontvangen?

- 1 keer
- 2 keer
- 3 keer
- Meer dan 3 keer

Vraag 12: Welke acties heb je ondernomen na het ontvangen van een phishing sms?

- Op de phishing link geklikt en ingelogd met mijn bankgegevens.
- Phishing sms verwijderd, telefoonnummer geblokkeerd.
- Phishing sms gemaild naar de bank.
- Phishing sms gemeld bij de politie.
- Geen actie ondernomen.

Vraag 13: Heb je uiteindelijk via de phishing link ingelogd met je bankgegevens?

- Ja
- Nee

Vraag 14: **Indien ja, wat zijn volgens jou de redenen waarom je hebt ingelogd met je bankgegevens?**

- Ik was niet bekend met het feit dat er phishing sms-berichten worden verstuurd.
- Ik heb de link niet gecheckt omdat de link op de webbrowser van smartphone niet geheel wordt weergegeven.
- Ik kreeg geen waarschuwing op mijn smartphone dat het om een valse website ging.

- Anders, namelijk:

Vraag 15: Indien je slachtoffer bent geworden van mobile phishing naar beveiligingscodes voor internetbankieren: Welke gevolgen heeft het voor jou gehad?

- Financiële gevolgen (bijvoorbeeld: het verlies van geld, verlies van je huis)
- Geestelijke gevolgen (bijvoorbeeld: verdriet, depressie, stress)
- Overige gevolgen (geen nadere toelichting)

Vraag 16: Hoeveel geld heb je ongeveer verloren door mobile phishing naar beveiligingscodes voor internetbankieren?

- 0-500 euro
- 500-1.000 euro
- 1000-3.000 euro
- 4.000-8.000 euro
- 8.000- 1.0000 euro
- Meer dan 1.000 euro

Vraag 17: Op welke wijze(n) zijn je inloggegevens op je smartphone beveiligd?

- 2-factor-authenticatie
- Vinger afdruk bij opvragen van inloggegevens
- Toegangscode
- Gezichtsherkenning
- Anders, namelijk
- Niet beveiligd

Vraag 18: Vind je dat je smartphone met je huidige mobiele beveiliging ook beveiligd is tegen mobile phishing naar beveiligingscodes voor internetbankieren?

- Ja
- Nee

Vraag 19: Heeft jouw bank je op de hoogte gesteld van dat criminelen zich voordoen als een bank of bekende instantie en phishing sms-berichten versturen?

- Ja
- Nee

Vraag 20: Stelling: Nederlandse banken zouden betere maatregelen moeten treffen om online bankieren te beveiligen.

Helemaal niet mee eens Neutraal Helemaal mee eens

Bijlage 4: Antwoorden Interview Nederlandse bank

1. Welke gevolgen heeft mobile phishing naar beveiligingscodes voor internetbankieren tot nu toe veroorzaakt bij de Rabobank?
   Uiteraard is het financiële plaatje een belangrijk aspect. Bij phishing naar beveiligingscodes lukt het de fraudeur in sommige gevallen ook om daadwerkelijk geld van de klant af te nemen. Situatieafhankelijk kan dit ook betekenen dat deze schade door de Rabobank wordt vergoed. Een gevolg is geweest dat we actief proberen te voorkomen dat onze klanten benadeelde worden van phishing.
   We waarschuwen onze klanten via verschillende communicatiekanalen om niet te reageren op phishingmails/sms'jes. Tevens hebben we een detectiemonitoringssysteem waarbij we verdachte transacties tijdig proberen te signaleren.
   We hebben uiteraard een zorgplicht tegenover onze klanten waar we zo goed mogelijk aan willen voldoen.
   1b Op welke wijze en langs welke kanalen wordt hierover gecommuniceerd?
   Denk hierbij aan berichten op:
   - www.Rabobank.nl
   - Twitter
   - Meldingen in de Rabobank App
   - Daarnaast wordt er soms met andere samengewerkt voor commercials op tv e.d.

2. Indien bekend, hoeveel bankklanten zijn tot nu toe slachtoffer geworden van mobile phishing naar beveiligingscodes voor internetbankieren bij de Rabobank?
   Ik kan de gegevens voor onze bank niet bekend maken. Ik adviseer je de landelijke cijfers van de Fraudehelpdesk te gebruiken. Het is uiteraard algemeen bekend dat mobile phishing nog in grote mate landelijk voorkomt en een groot probleem is.

3. Wat voert de Rabobank precies uit om de huidige bankklanten bewust te maken van deze vorm van mobile phishing?
   Zoals aangegeven proberen we herhaaldelijk bij onze klanten bewustwording te creëren. Bijvoorbeeld kunnen onze klanten informatie krijgen op onze website.
   Een voorbeeld hiervan: https://www.rabobank.nl/particulieren/veiligbankieren/phishing-vals-bericht-herkennen/

   Ook krijgen onze klanten regelmatig waarschuwingen pop-ups wanneer ze willen Internetbankieren.

   Verder is er ook samenwerking tussen de banken onderling om bijvoorbeeld middels commercials op tv aandacht te schenken aan dit onderwerp.

4. Welke beveiligingsmaatregelen treft de Rabobank om deze vorm van phishing tegen te gaan? Hoe wordt dit vormgegeven in de dagelijkse werkzaamheden en welke afdelingen houden zich hier mee bezig?
   We houden dagelijks bij wat de trends van deze vorm van fraude zijn. Hoe meer we weten inzake de wijze waarop de fraudeurs te werk gaan hoe meer gericht we hierop kunnen acteren.
   We hebben een specifieke fraudeafdeling die hier actief mee bezig is. We hebben diverse werkzaamheden die gericht zijn op de fase nadat een fraude heeft plaatsgevonden, maar een deel van de afdeling houdt zich ook actief bezig met het voorkomen van fraudes.
   Er is bijvoorbeeld een detectiesysteem die mogelijk frauduleuze transacties tijdig kan herkennen en op deze wijze is het vaak ook mogelijk om de schade tijdig te voorkomen. Over de ins en outs van dit systeem kan ik uiteraard niet veel bekend maken.

5. Hoe effectief denken jullie dat deze getroffen maatregelen zijn?
   Betreffende fraudevorm komt landelijk nog in grote mate voor. Ondanks dat er veel aandacht wordt besteed aan communicatie middels verschillende kanalen zijn er nog veel mensen die een betreffende fraudepoging niet tijdig herkennen en daadwerkelijk codes en andere gegevens afstaan.
   Ik denk dat de communicatie wel degelijk bijdraagt en ervoor zorgt dat er bij mensen sneller een belletje gaat rinkelen. Helaas zal er altijd een groep mensen zijn die ondanks de communicatie toch de betreffende fraudepoging niet herkennen en zodoende ook niet tijdig kunnen ingrijpen.

   Onze detectiesysteem draagt ook bij aan het tijdig detecteren van frauduleuze transacties. Dagelijks worden vele verdachte frauduleuze transacties tijdig gestopt, zodat schade wordt voorkomen. Ook hierbij geldt dat er ook nog veel frauduleuze transacties zijn die niet gestopt worden.

Bijlage 5: Plan voor verwerking van de resultaten

Hieronder is een plan beschreven van de verwerking van de enquête- en interviewresultaten.

1. **Enquêteresultaten**

De resultaten van de enquête zullen met behulp van statistieken, cijfers en tekst worden weergegeven. Overigens zal continu afgewogen worden of bepaalde data relevant is voor dit onderzoek. Dit wordt gedaan door te kijken of de data bijdragen aan het beantwoorden van de deelvragen van dit onderzoek. Data wat geen toegevoegde waarde heeft wordt weggelaten of in de bijlagen geplaatst.

Bij het verwerken van de resultaten van de enquête wordt gekeken naar welke enquête vragen bepaalde deelvragen dekken. Zie onderstaande tabel:

Deelvraag	**Enquête vraag**
6. Wat doen de eindgebruikers van smartphones zelf ter beveiliging van hun beveiligingscodes voor internetbankieren?	• Op welke wijze(n) zijn jouw inloggegevens op je smartphone beveiligd? • Vind je dat jouw smartphone met je huidige mobiele beveiliging ook beveiligd is tegen mobile phishing naar beveiligingscodes voor internetbankieren?
7. Welke oorzaken beïnvloeden slachtoffers om tijdens het gebruik van hun smartphone op een valse link te klikken en in te loggen met hun bankgegevens?	• Heb je ooit een soortgelijk phishing sms ontvangen? • Namens welke bank(en) of instantie(s) werd deze phishing sms verstuurd? • In welke periode(s) heb je een phishing sms ontvangen? • Welke acties heb je ondernomen na het ontvangen van een phishing sms? • Heb je uiteindelijk via de phishing link ingelogd met je bankgegevens? • Indien ja, wat zijn volgens jou de redenen waarom je hebt ingelogd met je bankgegevens?
8. In hoeverre zijn de maatregelen van banken om bankklanten te beschermen tegen mobile phishing naar beveiligingscodes voor internetbankieren bestand genoeg tegen mobile phishing naar beveiligingscodes voor internetbankieren?	• Heeft jouw bank je op de hoogte gesteld van dat criminelen zich voordoen als een bank of bekende instantie en phishing sms-berichten versturen? • Stelling: Nederlandse banken zouden betere maatregelen moeten treffen om online bankieren te beveiligen.

Overigens worden de volgende demografische kenmerken van de geënquêteerden beschreven: geslacht, leeftijd, opleidingsniveau en woonplaats. Er worden geen statistische toetsen toegepast om te bepalen of de eventuele verschillen tussen demografische groepen geënquêteerden significant zijn of op toeval berusten. De reden hiervan is omdat demografische kenmerken in de enquête waren opgenomen om te toetsten of deze invloed hebben op het slachtofferschap van mobile phishing. Echter zijn slechts drie van de 198 geënquêteerden slachtoffer geworden van mobile phishing. Dus het uitvoeren van een statistische toets is dan niet zinvol.

2. Resultaten semigestructureerde interviews

Er is een vragenlijst naar één medewerker van een Nederlandse bank gestuurd en deze is via de mail beantwoord. Uit de antwoorden zullen de belangrijkste uitspraken gehaald worden. Echter, omdat het om slechts één respondent gaat zullen de interviewantwoorden niet gecodeerd worden omdat er geen statistische analyse gedaan kan worden. De vragenlijst en de verkregen antwoorden zullen opgenomen worden in de bijlagen en in het rapport zal hiernaar verwezen worden. De naam van de respondent en de naam van de Nederlandse bank waar het om gaat zullen anoniem blijven.